Lead2pass-SY0-301

Number: SY0-301
Passing Score: 800
Time Limit: 120 min
File Version: 12.39

http://www.gratisexam.com/

Vendor: CompTIA

Exam Code: SY0-301

Exam Name: CompTIA Security+ Certification Exam

Version: 12.39

Important Notice

Product
Our Product Manager keeps an eye for Exam updates by Vendors. Free update is available within 150 days after your purchase.

You can login member center and download the latest product anytime. (Product downloaded from member center is always the latest.)

PS: Ensure you can pass the exam, please check the latest product in 2-3 days before the exam again.

Feedback
We devote to promote the product quality and the grade of service to ensure customers interest.

If you have any suggestions, please feel free to contact us support@lead2pass.com

If you have any questions about our product, please provide Exam Number, Version, Page Number, Question Number, and your Login Account to us, please contact us technology@lead2pass.com and our technical experts will provide support in 24 hours.

Copyright
The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will be inflicted legal punishment. We reserve the right of final explanation for this statement.
CompTIA SY0-301 Exam

Exam A

QUESTION 1
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

QUESTION 2
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

QUESTION 3
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

QUESTION 4
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

QUESTION 5
"First Test, First Pass" - www.lead2pass.com 4
CompTIA SY0-301 Exam

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

QUESTION 6
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

QUESTION 7
Isolation mode on an AP provides which of the following functionality types?

A. Segmentation of each wireless user from other wireless users
B. Disallows all users from communicating directly with the AP
C. Hides the service set identifier
D. Makes the router invisible to other routers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Employees are reporting that unauthorized personnel are in secure areas of the building. This is MOST likely due to lack of security awareness in which of the following areas?

A. Impersonation
B. Logical controls
C. Physical security controls
D. Access control policy

Correct Answer: C
Section: (none)
Explanation

QUESTION 9
A forensic image of a hard drive has been created. Which of the following can be used to demonstrate the image has not been tampered with?

A. Chain of custody
B. Document the image file's size and time stamps
C. Encrypt the image file
D. Hash of the image file
"First Test, First Pass" - www.lead2pass.com 5
CompTIA SY0-301 Exam

Correct Answer: D
Section: (none)
Explanation

QUESTION 10
Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 11
Which of the following security concepts can Matt, a security administrator, implement to support integrity?

A. Digital signatures
B. Trust models
C. Key escrow
D. Recovery agents

Correct Answer: A
Section: (none)
Explanation

QUESTION 12
Which of the following combinations represents multifactor authentication?

A. Smart card and hard token
B. Voice print analysis and facial recognition
C. Username and PIN
D. Cipher lock combination and proximity badge

Correct Answer: D
Section: (none)
Explanation

QUESTION 13
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

QUESTION 14

Which of the following is Jane, a security administrator, MOST likely implementing when deleting all the unneeded files and modules of a newly installed application?

A. Exception handling
B. Patch management
C. System file clean up
D. Application hardening

Correct Answer: D
Section: (none)
Explanation

QUESTION 15
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

QUESTION 16
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

QUESTION 17
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

QUESTION 18
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

QUESTION 19
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

QUESTION 20
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

QUESTION 21
Which of the following is MOST likely to result in data loss?

A. Accounting transferring confidential staff details via SFTP to the payroll department
B. Back office staff accessing and updating details on the mainframe via SSH
C. Encrypted backup tapes left unattended at reception for offsite storage
D. Developers copying data from production to the test environments via a USB stick

Correct Answer: D
Section: (none)
Explanation

QUESTION 22
Sara, a security administrator, sends an email to the user to verify their password has been reset. Which of the following threats is BEST mitigated by this action?

A. Spear phishing
B. Impersonation
C. Hoaxes
D. Evil twin

Correct Answer: B
Section: (none)
Explanation

QUESTION 23

Which of the following describes an LDAP injection attack?

A. Creating a copy of user credentials during the LDAP authentication session
B. Manipulating an application's LDAP query to gain or alter access rights
C. Sending buffer overflow to the LDAP query service
D. Using XSS to direct the user to a rogue LDAP server

Correct Answer: B
Section: (none)
Explanation

QUESTION 24
Which of the following concepts defines the requirement for data availability?

A. Authentication to RADIUS
B. Non-repudiation of email messages
C. Disaster recovery planning
D. Encryption of email messages

Correct Answer: C
Section: (none)
Explanation

QUESTION 25
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

QUESTION 26
Which of the following is an attack designed to steal cell phone data and contacts?

A. Bluesnarfing
B. Smurfing
C. Fuzzing
D. Bluejacking

Correct Answer: A
Section: (none)
Explanation

QUESTION 27
Which of the following best practices is commonly found at the end of router ACLs?

A. Time of day restrictions

B. Implicit deny
C. Implicit allow
D. Role-based access controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 9
CompTIA SY0-301 Exam

QUESTION 28
Which of the following uses TCP / UDP port 53 by default?

A. DNS
B. SFTP
C. SSH
D. NetBIOS

Correct Answer: A
Section: (none)
Explanation

QUESTION 29
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning
B. Quantitative assessment
C. Data classification
D. Qualitative assessment

Correct Answer: C
Section: (none)
Explanation

QUESTION 30
Sara, the network administrator, was alerted to an unauthorized email that was sent to specific VIPs in the company with a malicious attachment. Which of the following types of attacks is MOST likely being described?

A. Vishing
B. Whaling
C. DDoS
D. Pharming

Correct Answer: B
Section: (none)
Explanation

QUESTION 31

In the event of a mobile device being lost or stolen, which of the following BEST protects against sensitive information leakage?

A. Cable locks
B. Remote wipe
C. Screen lock
D. Voice encryption

Correct Answer: B
Section: (none)
Explanation

QUESTION 32
Which of the following should Sara, a security administrator, perform periodically to reduce an

organization's risk exposure by verifying employee access?

A. Account revalidation
B. Incident management
C. Qualitative analysis
D. Quantitative analysis

Correct Answer: A
Section: (none)
Explanation

QUESTION 33
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Correct Answer: A
Section: (none)
Explanation

QUESTION 34
Which of the following is MOST appropriate when storing backup tapes in a physically non-secure room?

A. Use an in-tape GPS tracking device.
B. Store the tapes in a locked safe.
C. Encrypt the tapes with AES.
D. Securely wipe the tapes.

Correct Answer: B
Section: (none)

Explanation

QUESTION 35
Grandfather-Father-Son and Tower of Hanoi are common:

A. Trojans that collect banking information.
B. Backup tape rotation strategies.
C. Penetration testing best practices.
D. Failover practices in clustering.

Correct Answer: B
Section: (none)
Explanation

QUESTION 36
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

QUESTION 37
Which of the following can BEST be implemented on a mobile phone to help prevent any sensitive data from being recovered if the phone is lost?

A. Voice encryption
B. Screen locks
C. Device encryption
D. GPS tracking

Correct Answer: C
Section: (none)
Explanation

QUESTION 38
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

QUESTION 39
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

QUESTION 40
Which of the following is BEST associated with PKI?

A. Private key
B. Block ciphers
C. Stream ciphers
D. NTLMv2

Correct Answer: A
Section: (none)
Explanation

QUESTION 41
"First Test, First Pass" - www.lead2pass.com 12
CompTIA SY0-301 Exam

Which of the following malware types is BEST described as protecting itself by hooking system processes and hiding its presence?

A. Botnet
B. Rootkit
C. Logic bomb
D. Virus

Correct Answer: B
Section: (none)
Explanation

QUESTION 42
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

QUESTION 43
Following a security failure incident, the chain of custody must be followed in order to:

A. Determine who accessed the compromised equipment pre-incident.
B. Securely lock down any compromised equipment.
C. Preserve and maintain evidence integrity.
D. Provide an accurate timeline detailing how the incident occurred.

Correct Answer: C
Section: (none)
Explanation

QUESTION 44
Jane, an IT administrator, is implementing security controls on a Microsoft Windows based kiosk used at a bank branch. This kiosk is used by the public for Internet banking. Which of the following controls will BEST protect the kiosk from general public users making system changes?

A. Group policy implementation
B. Warning banners
C. Command shell restrictions
D. Host based firewall

Correct Answer: A
Section: (none)
Explanation

QUESTION 45
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

QUESTION 46
The corporate NIPS requires a daily download from its vendor with updated definitions in order to block the latest attacks. Which of the following describes how the NIPS is functioning?

A. Heuristics
B. Anomaly based
C. Signature based
D. Behavior based

Correct Answer: C
Section: (none)
Explanation

QUESTION 47
Pete, a security administrator, needs to update the community strings on the router since they have been compromised. Which of the following needs to be changed?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 48
Which of the following authentication services uses the AAA architecture and runs on TCP?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 49
Users have notified Sara, a technician, that the performance of a specific set of servers has degraded. All of the servers are in the same facility and accessible, but are very slow to respond.
Which of the following is MOST likely the cause?

A. The servers are not configured in a hot aisle and cool aisle containment.
B. Redundancy and data de-duplication has failed.

C. The UPS is overloaded and has begun the shutdown process.
D. HVAC has failed causing server CPUs to overheat and throttle.

Correct Answer: D
Section: (none)
Explanation

QUESTION 50
Matt, an administrator, captures malicious DNS traffic on the network. Which of the following tools would be used to analyze the nature of this traffic?

A. Sniffer
B. Zone transfer
C. Network tap
D. Application firewall

Correct Answer: A
Section: (none)
Explanation

QUESTION 51
Which of the following explains the difference between a public key and a private key?

A. The public key is only used by the client while the private key is available to all. Both keys are mathematically related.
B. The private key only decrypts the data while the public key only encrypts the data. Both keys are mathematically related.
C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
D. The private key is only used by the client and kept secret while the public key is available to all.

Correct Answer: D
Section: (none)
Explanation

QUESTION 52
User A is a member of the payroll security group. Each member of the group should have read/write permissions to a share. User A was trying to update a file but when the user tried to access the file the user was denied. Which of the following would explain why User A could not access the file?

A. Privilege escalation
B. Rights are not set correctly
C. Least privilege
D. Read only access

Correct Answer: B
Section: (none)
Explanation

QUESTION 53
A technician is implementing a new wireless network for an organization. The technician should be concerned with all of the following wireless vulnerabilities EXCEPT:

A. rogue access points.

B. 802.11 mode.
"First Test, First Pass" - www.lead2pass.com 15
CompTIA SY0-301 Exam
C. weak encryption.
D. SSID broadcasts.

Correct Answer: B
Section: (none)
Explanation

QUESTION 54
An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns. Which of the following is an example of this threat?

A. An attacker using the phone remotely for spoofing other phone numbers
B. Unauthorized intrusions into the phone to access data
C. The Bluetooth enabled phone causing signal interference with the network
D. An attacker using exploits that allow the phone to be disabled

Correct Answer: B
Section: (none)
Explanation

QUESTION 55
An administrator wants to block users from accessing a few inappropriate websites as soon as possible. The existing firewall allows blocking by IP address. To achieve this goal the administrator will need to:

A. upgrade to a DNS based filter to achieve the desired result.
B. use the company AUP to achieve the desired result.
C. upgrade to a URL based filter to achieve the desired result.
D. upgrade to a text based filter to achieve the desired result.

Correct Answer: C
Section: (none)
Explanation

QUESTION 56
An administrator wishes to deploy an IPSec VPN connection between two routers across a WAN. The administrator wants to ensure that the VPN is encrypted in the most secure fashion possible. Which of the following BEST identifies the correct IPSec mode and the proper configuration?

A. IPSec in tunnel mode, using both the ESP and AH protocols
B. IPSec in tunnel mode, using the ESP protocol
C. IPSec in transport mode, using the AH protocol
D. IPSec in transport mode, using both ESP and AH protocols

Correct Answer: A
Section: (none)
Explanation

QUESTION 57

An administrator has just performed an audit on their network. The security administrator has not allowed the results to be shown to the IT departmental staff. Which of the following BEST describes the reasoning for this?

A. Least privilege
B. Job rotation
C. Separation of duties
D. Implicit deny
"First Test, First Pass" - www.lead2pass.com 16
CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

QUESTION 58
Which of the following is the primary objective of a business continuity plan (BCP)?

A. Addresses the recovery of an organizations business operations
B. Addresses the recovery of an organizations business payroll system
C. Addresses the recovery of an organizations business facilities
D. Addresses the recovery of an organizations backup site

Correct Answer: A
Section: (none)
Explanation

QUESTION 59
A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If determining the risk, which of the following is the annual loss expectancy (ALE)?

A. $2,700
B. $4,500
C. $5,000
D. $7,290

Correct Answer: D
Section: (none)
Explanation

QUESTION 60
All of the following are organizational policies that reduce the impact of fraud EXCEPT:

A. separation of duties.
B. password complexity rules.
C. job rotation.
D. escorting procedures.

Correct Answer: B

Section: (none)
Explanation

QUESTION 61
Which of the following features would allow Pete, a network administrator, to allow or deny access to a specific list of network clients?

A. Content filtering
B. Flood guard
C. URL filtering
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 17
CompTIA SY0-301 Exam

QUESTION 62
Pete, a system administrator, is using a packet sniffer to troubleshoot remote authentication. Pete detects a device trying to communicate to UDP ports 1812 and 1813. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 63
Which of the following is an example of authentication using something Jane, a user, has and something she knows?

A. GSM phone card and PIN
B. Username and password
C. Username and PIN
D. Fingerprint scan and signature

Correct Answer: A
Section: (none)
Explanation

QUESTION 64
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

QUESTION 65
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

QUESTION 66
Which of the following does Jane, a software developer, need to do after compiling the source code of a program to attest the authorship of the binary?

A. Place Jane's name in the binary metadata
B. Use Jane's private key to sign the binary
C. Use Jane's public key to sign the binary
D. Append the source code to the binary

Correct Answer: B
Section: (none)
Explanation

QUESTION 67
During the analysis of malicious code, Matt, a security analyst, discovers JavaScript being used to send random data to another service on the same system. This is MOST likely an example of which of the following?

A. Buffer overflow
B. XML injection
C. SQL injection
D. Distributed denial of service

Correct Answer: A
Section: (none)
Explanation

QUESTION 68

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

QUESTION 69
A company's backup solution performs full backups weekly and is running into capacity issues. Without changing the frequency of backups, which of the following solutions would reduce the storage requirement?

A. Differential backups
B. Magnetic media backups
C. Load balancing
D. Incremental backups

Correct Answer: D
Section: (none)
Explanation

QUESTION 70
3DES is created when which of the following scenarios occurs?

A. The DES algorithm is run three consecutive times against the item being encrypted.
B. The DES algorithm has been used by three parties: the receiving party, sending party, and "First Test, First Pass" - www.lead2pass.com 19
CompTIA SY0-301 Exam
server.
C. The DES algorithm has its key length increased to 256.
D. The DES algorithm is combined with AES and SHA1.

Correct Answer: A
Section: (none)
Explanation

QUESTION 71
Which of the following mitigates the risk of proprietary information being compromised?

A. Cloud computing
B. Digital signatures
C. File encryption
D. Virtualization

Correct Answer: C
Section: (none)
Explanation

QUESTION 72
Which of the following security tools can Jane, an administrator, implement to mitigate the risks of theft?

A. Virtualization
B. Host based firewalls
C. HIPS
D. Device encryption

Correct Answer: D
Section: (none)
Explanation

QUESTION 73
Matt, an attacker, drops a USB flash drive labeled "CEO's music collection" in the reception area of a bank hoping an employee will find it. The drive actually contains malicious code. Which of the following attacks is this?

A. Vishing
B. Social engineering
C. Spim
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

QUESTION 74
Sara, an employee, visits a website and downloads the PDF application to officially become a member. The network administrator notices large amounts of bandwidth at night from Sara's workstation. Which of the following attacks does this describe?

A. Adware
B. Botnets
C. Logic bomb
D. Spyware

Correct Answer: B
Section: (none)
Explanation

QUESTION 75
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

QUESTION 76
If Pete, an administrator, is blocking port 22, which of the following protocols will this affect? (Select TWO)

A. SNMP
B. SSH
C. SMTP
D. FTP
E. Telnet
F. SCP

Correct Answer: BF
Section: (none)
Explanation

QUESTION 77
Which of the following allows active exploitation of security vulnerabilities on a system or network for the purpose of determining true impact?

A. Port scanning
B. Penetration testing
C. Vulnerability scanning
D. Performing risk analysis

Correct Answer: B
Section: (none)
Explanation

QUESTION 78
Which of the following web application security weaknesses can be mitigated by preventing the use of HTML tags?

A. LDAP injection
B. SQL injection

C. Error and exception handling
D. Cross-site scripting

Correct Answer: D
Section: (none)
Explanation

QUESTION 79

A recent virus outbreak has finally been contained and now several users are reporting latency issues. A vulnerability scan was performed and no backdoors were found. Upon further investigation, Matt, the security administrator, notices that websites are being redirected to unauthorized sites. This is an example of which of the following?

A. Botnet
B. Rootkits
C. Trojan
D. Spyware

Correct Answer: D
Section: (none)
Explanation

QUESTION 80
Which of the following is BEST used to control access to the LAN?

A. DMZ
B. NAC
C. NAT
D. Remote access

Correct Answer: B
Section: (none)
Explanation

QUESTION 81
Which of the following is a technical preventive control?

A. IDS
B. Data backup
C. Audit logs
D. ACLs

Correct Answer: D
Section: (none)
Explanation

QUESTION 82
When deploying virtualized servers, which of the following should a company be the MOST concerned with?

A. Integrity
B. Non-repudiation
C. Power consumption
D. Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
The main difference between symmetric and asymmetric encryption is that:

A. Symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses one key to encrypt and one to decrypt.
B. In symmetric encryption the encryption key must be of even number length so that it can be split in two, where one part is used for encryption and the other is used for decryption.
C. Asymmetric encryption uses the same key for encryption and decryption, while symmetric encryption uses one key to encrypt and one to decrypt.
D. In asymmetric encryption the same key is given to one user in a hashed format and used for encryption, and to another used in plain text and used for decryption "Pass Any Exam. Any Time." - www.actualtests.com 53 CompTIA SY0-301 Exam

Correct Answer: A
Section: (none)
Explanation

QUESTION 84
Jane, an information security manager, often receives reports about the sharing of cipher lock codes to gain access to secure areas. Jane would like to implement a new control that would prevent the sharing of codes and limit access points to only key employees. Which of the following security controls would BEST mitigate this issue?

A. Use ACLs
B. Separation of duties
C. Install proximity readers
D. Time of day restrictions

Correct Answer: C
Section: (none)
Explanation

QUESTION 85
Jane, a security administrator, has been tasked with explaining access control aspects to a peer. Which of the following is a directory service supporting both Windows and Linux authentication?

A. LDAP
B. Trusted OS
C. TACACS+
D. PAM

Correct Answer: A
Section: (none)
Explanation

QUESTION 86
Pete, a system administrator, has concerns regarding his users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.
B. Enforce a policy shortening the credential expiration timeframe.

C. Implement biometric readers on laptops and restricted areas.
D. Install security cameras in areas containing sensitive systems.

Correct Answer: C
Section: (none)
Explanation

QUESTION 87
Which of the following is the MOST secure solution for connecting remote sites to the corporate headquarters?

A. PPTP
B. L2TP
C. HTTP
D. IPSec

Correct Answer: D
Section: (none)
Explanation

QUESTION 88
Which of the following is the BEST method to use when preventing a cross-site scripting attack on a Human Resource system?

A. Require all data be filtered through a web application firewall.
B. Restrict permitted HTML encoding to a limited subset of tags and attributes.
C. Provide user education on the threat of cross-site scripting.
D. Input validation upon arrival at the server.

Correct Answer: D
Section: (none)
Explanation

QUESTION 89
Jane's, a user, word processing software is exhibiting strange behavior, opening and closing itself at random intervals. There is no other strange behavior on the system. Which of the following would mitigate this problem in the future?

A. Install application updates
B. Encrypt the file system
C. Install HIDS
D. Install anti-spam software

Correct Answer: A
Section: (none)
Explanation

QUESTION 90
Jane, a user, has an IP address of 172.16.24.43 and visits a website which states that she has an IP address of 204.211.38.89. Which of the following is being used on the network? (Select TWO).

A. NAT
B. NAC
C. Spoofing
D. DMZ
E. VLANs
F. PAT

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 24
CompTIA SY0-301 Exam

QUESTION 91
Which of the following data loss prevention strategies mitigates the risk of replacing hard drives that cannot be sanitized?

A. Virtualization
B. Patch management
C. Full disk encryption
D. Database encryption

Correct Answer: C
Section: (none)
Explanation

QUESTION 92
Which of the following is characterized by Matt, an attacker, attempting to leave identification markings for open wireless access points?

A. Initialization vector
B. War chalking
C. Packet sniffing
D. War driving

Correct Answer: B
Section: (none)
Explanation

QUESTION 93
Which of the following can Matt, a security administrator, implement to support confidentiality and integrity?

A. PKI
B. Non-repudiation
C. Digital signatures
D. Recovery agents

Correct Answer: A
Section: (none)

Explanation

QUESTION 94
Which of the following can Pete, an administrator, use to verify that a downloaded file was not corrupted during the transfer?

A. NTLM tag
B. LANMAN hash
C. MD5 checksum
D. SHA summary

Correct Answer: C
Section: (none)
Explanation

QUESTION 95
Planning what traffic will be separated, assigning tags, and configuring routing are part of configuring which of the following?

A. IPSec
B. ACL
C. NAT
D. VLAN

Correct Answer: D
Section: (none)
Explanation

QUESTION 96
Jane, an employee, receives an error on an encrypted laptop, making the laptop un-bootable. Jane now cannot access any files on the laptop. The desktop technician is unable to recover the key from the computer and will have to inform Jane that the files are now unrecoverable. Which of the following would have prevented Jane from losing access to the files?

A. Certificate Authority
B. Private keys
C. Public keys
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

QUESTION 97
Which of the following combines authentication and authorization, and does not use the TCP protocol?

A. RADIUS
B. Kerberos

C. LDAP
D. TACACS+

Correct Answer: A
Section: (none)
Explanation

QUESTION 98
Which of the following occurs when two access points share the same SSID broadcast where one access point is used to capture data?

A. Rogue access point
B. Bluesnarfing
C. Evil twin
D. Packet sniffing

Correct Answer: C
Section: (none)
Explanation

QUESTION 99
Pete and Jane, users in a financial office are reporting that they are not being asked for credentials anymore when successfully connecting to the company wireless. All other offices are still being authenticated on the wireless. Which of the following is this an example of?

A. Evil twin
B. Interference

C. IV attack
D. War driving

Correct Answer: A
Section: (none)
Explanation

QUESTION 100
Which of the following is BEST described by a scenario where management chooses to implement security controls to lessen the impact of a given risk?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 101
A recent network attack caused several random computers to malfunction, even though those computers had

the latest updates and patches applied. Which of the following describes this type of attack?

A. Targeted
B. DDoS
C. Zero day
D. Buffer overflow

Correct Answer: C
Section: (none)
Explanation

QUESTION 102
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

QUESTION 103
Sara makes a phone call to the help desk pretending to be Jane. Sara states that she has forgotten her password and asks that it be reset to 12345. Which of the following is Sara performing?

A. Shoulder surfing
B. Impersonation
C. Dumpster diving

D. Tailgating

Correct Answer: B
Section: (none)
Explanation

QUESTION 104
Which of the following default network ports is used by FTP?

A. 20
B. 22
C. 23
D. 25

Correct Answer: A
Section: (none)
Explanation

QUESTION 105
A company recently installed a load balancer for their servers. The company is MOST concerned with:

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 106
Which of the following pseudocodes MOST likely prevents buffer overflows?

A. If input contains < or > then escape the character and execute the program with user input
B. If input is less than 100 characters, then prompt for input again
C. If input contains \ then remove \ and execute program with user input
D. If input is greater than 1000 characters then truncate input

Correct Answer: D
Section: (none)
Explanation

QUESTION 107
Which of the following is usually encrypted when stored or transmitted?

A. CRL
B. Private key
C. Root certificate
D. Public key

Correct Answer: B
Section: (none)
Explanation

QUESTION 108
Which of the following could Jane, a security administrator, implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.
B. Only allow employees to enter or leave through one door at specified times of the day.
C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
D. Train employees on risks associated with social engineering attacks and enforce policies.

Correct Answer: D
Section: (none)
Explanation

QUESTION 109
Pete, a security administrator, implemented design changes and moved certain servers into a dedicated area that is accessible from the outside network, yet separated from the internal network. Which of the following did Pete implement?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 110
While placing an order at an online bookstore, Sara, a user, enters her correct credentials and is immediately presented with a pop-up window requesting her username and password again.
Which of the following has MOST likely occurred?

A. LDAP injection attack
B. Evil twin attack
C. Phishing attack
D. SQL injection attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 111
Identifying a list of all approved software on a system is a step in which of the following practices?

A. Passively testing security controls
B. Application hardening
C. Host software baselining
D. Client-side targeting

Correct Answer: C
Section: (none)
Explanation

QUESTION 112
Pete, an administrator, captures traffic sent between a router and a monitoring server on port 161. The packet payload contains the strings 'PUBLIC and 'PRIVATE1. Which of the following was MOST likely used to capture this traffic?

A. Vulnerability scanner

B. Protocol analyzer
C. SNMPv3

D. SNMPv2c

Correct Answer: B
Section: (none)
Explanation

QUESTION 113
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

QUESTION 114
Which of the following malware types typically allows Pete, 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

QUESTION 115
Which of the following BEST describes a common security concern for cloud computing?

A. Data may be accessed by third parties who have compromised the cloud platform
B. Antivirus signatures are not compatible with virtualized environments
C. Network connections are too slow
D. CPU and memory resources may be consumed by other servers in the same cloud

Correct Answer: A
Section: (none)
Explanation

QUESTION 116
Which of the following is the MOST secure authentication protocol?

A. CHAP
B. PEAP
C. EAP
D. LEAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 30
CompTIA SY0-301 Exam

QUESTION 117
Which of the following policies could be implemented to help prevent users from displaying their login credentials in open view for everyone to see?

A. Privacy
B. Clean desk
C. Job rotation
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

QUESTION 118
Which of the following should Sara, a security technician, create to articulate the requirements for what is and what is not condoned on company systems?

A. Acceptable usage policy
B. Retention policy
C. Privacy policy
D. Access control policy

Correct Answer: A
Section: (none)
Explanation

QUESTION 119
Users have reported that when they go to the company website they are sent to a competitor's site instead. Which of the following is the MOST likely explanation?

A. Someone has employed ARP poisoning against the company.
B. Someone has employed DNS poisoning against the company.
C. Someone has accidentally unplugged the company's web server.
D. The competitor has a more powerful web server.

Correct Answer: B
Section: (none)
Explanation

QUESTION 120
Sara, an IT Administrator, wants to make sure that only certain devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

A. MAC filtering

B. Increase the power levels of the WAP
C. Dynamic DHCP
D. Disable SSID broadcast

Correct Answer: A
Section: (none)
Explanation

QUESTION 121
Which of the following is BEST used to determine the source of a network bottleneck?

A. Sniffer
B. Router

C. Firewall
D. Switch

Correct Answer: A
Section: (none)
Explanation

QUESTION 122
Sara, a system administrator, installed new database software and notices that after running port scan on the server port 21 is now open. The database does not use any type of file transfer program. Which of the following would reduce the amount of unnecessary services being used?

A. NIPS
B. Application hardening
C. NIDS
D. Application base lining

Correct Answer: B
Section: (none)
Explanation

QUESTION 123
Matt, the administrator, spots a sustained spike in disk activity and CPU utilization; network activity looks normal. Which of the following might this indicate?

A. This server is now a member of a botnet.
B. There is a virus infecting the server.
C. There is a smurf attack occurring on the server.
D. Users are copying more files from the server than normal.

Correct Answer: B
Section: (none)
Explanation

QUESTION 124
Matt, the security administrator, has changed the default settings on a Web server, removing certain files and

directories. This is an example of which of the following?

A. Application configuration baseline
B. Application hardening
C. Cross-site scripting prevention
D. Application patch management

Correct Answer: B
Section: (none)
Explanation

QUESTION 125
Biometrics includes the use of which of the following authentication methods?

A. Single sign-on
B. Retinal scan
C. Common access card
D. ACLs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 32
CompTIA SY0-301 Exam

QUESTION 126
Pete, the security administrator, wants to implement password controls to mitigate attacks based on password reuse. Which of the following password controls used together BEST accomplishes this? (Select TWO).

A. Minimum password age and password history
B. Password complexity and password history
C. Password history and password expiration
D. Password complexity and password expiration
E. Maximum password age and password expiration

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A company that trains their users to lock the doors behind them is MOST likely trying to prevent:

A. Vishing attacks
B. Dumpster diving
C. Shoulder surfing
D. Tailgating

Correct Answer: D
Section: (none)
Explanation

QUESTION 128
Which of the following security controls would be applied on individual hosts to monitor suspicious activities, by actively analyzing events occurring within that host, and blocking any suspicious or abnormal activity?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 129
Jane, a security administrator, forgets his card to access the server room. Jane asks Matt if she could use his card for the day. Which of the following is Jane using to gain access to the server room?

A. Man-in-the-middle
B. Tailgating
C. Impersonation
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

QUESTION 130

During a forensic investigation, which of the following information is compared to verify the contents of a hard drive image match the original drive and have not been changed by the imaging process?

A. Hash values
B. Chain of custody
C. Order of volatility
D. Time offset

Correct Answer: A
Section: (none)
Explanation

QUESTION 131
Jane brought a laptop in from home and connected the Ethernet interface on the laptop to a wall jack with a patch cable. Jane was unable to access any network resources. Which of the following is the MOST likely cause?

A. Flood guards were enabled on the switch.
B. Loop protection prevented the laptop from accessing the network.
C. Port security was enabled on the switch.
D. Router access control lists prevented the laptop from accessing the network.

Correct Answer: C
Section: (none)
Explanation

QUESTION 132
Matt, a new employee, installed an application on his workstation that allowed Internet users to have access to his workstation. Which of the following security related training could have mitigated this action?

A. Use of proper password procedures
B. Use of personally owned devices
C. Use of social networking and P2P networks
D. Use of clean desk policies

Correct Answer: C
Section: (none)
Explanation

QUESTION 133
Which of the following threats can result from a lack of controls for personal webmail?

A. Bandwidth exhaustion
B. Cross-site request forgery
C. Data leakage
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

QUESTION 134
Which of the following is identified by the command: INSERT INTO users ("admin", "admin");'?

A. SQL Injection
B. Directory traversal
C. LDAP injection
D. Session hijacking

Correct Answer: A

Section: (none)
Explanation

QUESTION 135
Which of the following attacks is MOST likely to be performed against an FTP server?

A. DLL injection
B. SQL injection
C. LDAP injection
D. Command injection

Correct Answer: D
Section: (none)
Explanation

QUESTION 136
After performing a port scan, Sara, a network administrator, observes that port 443 is open. Which of the following services is MOST likely running?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 137
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

QUESTION 138
Matt, a security administrator, conducted a scan and generated a vulnerability report for the Chief Executive Officer (CEO). The vulnerability report indicated several vulnerabilities but the CEO has decided that cost and operational impact outweigh the risk. This is an example of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 139
A good password policy should contain which of the following rules? (Select THREE)

A. Length
B. Expiration
C. Tokens
D. Smart card
E. Enrollment
F. Complexity
G. Biometrics

Correct Answer: ABF
Section: (none)
Explanation

QUESTION 140
Jane, a security administrator, identifies a WEP-encrypted WAP on the network that is located at the end of the building. Jane has noticed that it is the most utilized WAP on the network. When trying to manage the WAP, she is unable to gain access. Which of the following has MOST likely happened to the WAP?

A. The WAP is under an IV attack
B. The WAP's MAC address has been spoofed
C. The WAP is a rogue access point
D. The WAP was victim to a bluejacking attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 141
Jane, a human resources employee, receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 142
A network IPS is used for which of the following?

A. To identify and document network based intrusions and network traffic
B. To document and analyze network visualization threats and performance
C. To identify and prevent network based intrusions or unwanted network traffic
D. To document and analyze malware and viruses on the Internet "First Test, First Pass" - www.lead2pass.com 36
CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

QUESTION 143
A risk is identified that an attacker, given the right credentials, could potentially connect to the corporate network from a nearby business's parking lot. Which of the following controls can be put in place to reduce the likelihood of this occurring? (Select TWO).

A. TKIP
B. Antenna placement
C. Power level controls
D. WPA
E. WPA2
F. Disable SSID broadcasting

Correct Answer: BC
Section: (none)
Explanation

QUESTION 144
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

QUESTION 145
Sara, an administrator, is hardening email application communication to improve security. Which of the following could be performed?

A. Remove gateway settings from the route table
B. Password protect the server BIOS
C. Disabling high I/O services
D. Require TLS when using SMTP

Correct Answer: D
Section: (none)

Explanation

QUESTION 146
Which of the following increases proper airflow in a datacenter?

A. Humidity controls
B. Video monitoring
C. Temperature controls
D. Hot and cold aisles

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 37
CompTIA SY0-301 Exam

QUESTION 147
Jane, an IT security technician, needs to create a way to secure company mobile devices. Which of the following BEST meets this need?

A. Implement voice encryption, pop-up blockers, and host-based firewalls.
B. Implement firewalls, network access control, and strong passwords.
C. Implement screen locks, device encryption, and remote wipe capabilities.
D. Implement application patch management, antivirus, and locking cabinets.

Correct Answer: C
Section: (none)
Explanation

QUESTION 148
In which of the following orders should Jane, an administrator, capture a system's data for forensics investigation?

A. Hard disk, swap file, system memory, CPU cache
B. CPU cache, system memory, swap file, hard disk
C. System clock, flash BIOS, memory, hard disk
D. Flash BIOS, system memory, swap file, hard disk

Correct Answer: B
Section: (none)
Explanation

QUESTION 149
In PKI, a key pair consists of:

A. A key ring
B. A public key
C. A private key
D. Key escrow
E. A passphrase

Correct Answer: BC
Section: (none)
Explanation

QUESTION 150
Which of the following would MOST likely ensure that swap space on a hard disk is encrypted?

A. Database encryption
B. Full disk encryption
C. Folder and file encryption
D. Removable media encryption

Correct Answer: B
Section: (none)
Explanation

QUESTION 151
Why would a technician use a password cracker?

A. To look for weak passwords on the network
B. To change a users passwords when they leave the company "First Test, First Pass" - www.lead2pass.com 38
CompTIA SY0-301 Exam
C. To enforce password complexity requirements
D. To change users passwords if they have forgotten them

Correct Answer: A
Section: (none)
Explanation

QUESTION 152
An application developer is looking for an encryption algorithm which is fast and hard to break if a large key size is used. Which of the following BEST meets these requirements?

A. Transposition
B. Substitution
C. Symmetric
D. Asymmetric

Correct Answer: C
Section: (none)
Explanation

QUESTION 153
Which of the following is the MOST common logical access control method?

A. Access control lists
B. Usernames and password
C. Multifactor authentication
D. Security ID badges

Correct Answer: B
Section: (none)
Explanation

QUESTION 154
Which of the following are reasons to implement virtualization technology? (Select TWO).

A. To reduce recovery time in the event of application failure
B. To decrease false positives on the NIDS
C. To eliminate virtual redundancy
D. To decrease access to security resources
E. To provide a secure virtual environment for testing

Correct Answer: AE
Section: (none)
Explanation

QUESTION 155
A botnet zombie is using HTTP traffic to encapsulate IRC traffic. Which of the following would detect this encapsulated traffic?

A. Vulnerability scanner
B. Proxy server
C. Anomaly-based IDS
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 39
CompTIA SY0-301 Exam

QUESTION 156
Which of the following allows an attacker to manipulate files by using the least significant bit(s) to secretly embed data?

A. Steganography
B. Worm
C. Trojan horse
D. Virus

Correct Answer: A
Section: (none)
Explanation

QUESTION 157
Which of the following is the BEST way to mass deploy security configurations to numerous workstations?

A. Security hotfix

B. Configuration baseline
C. Patch management
D. Security templates

Correct Answer: D
Section: (none)
Explanation

QUESTION 158
Which of the following should be included in a forensic toolkit?

A. Compressed air
B. Tape recorder
C. Fingerprint cards
D. Digital camera

Correct Answer: D
Section: (none)
Explanation

QUESTION 159
After a period of high employee turnover, which of the following should be implemented?

A. A review of NTLM hashes on the domain servers
B. A review of group policies
C. A review of user access and rights
D. A review of storage and retention policies

Correct Answer: C
Section: (none)
Explanation

QUESTION 160
Which of the following may be an indication of a possible system compromise?

A. A port monitor utility shows that there are many connections to port 80 on the Internet facing web server.
B. A performance monitor indicates a recent and ongoing drop in speed, disk space or memory utilization from the baseline.

C. A protocol analyzer records a high number of UDP packets to a streaming media server on the Internet.
D. The certificate for one of the web servers has expired and transactions on that server begins to drop rapidly.

Correct Answer: B
Section: (none)
Explanation

QUESTION 161
Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?

A. Chain of custody
B. Tracking man hours
C. Witnesses
D. Capturing system images

Correct Answer: A
Section: (none)
Explanation

QUESTION 162
Ticket-Granting-Tickets (TGTs) are common in which of the following authentication schemes?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 163
Sara, a security administrator, implemented design changes which allowed for greater availability of IP addresses. Which of the following did Sara implement?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 164
Jane, an IT security administrator, is attempting to implement PKI within her organization. Which of the following BEST explains why the company needs PKI?

A. The company needs PKI because the organization is based on trust models with many external organizations.
B. The company needs PKI because they need the ability to encrypt messages with centralized verification.
C. The company needs PKI because there is insufficient key escrow for outsourced SSL certificates.

D. The company needs PKI because it only has one recovery agent within the company.

Correct Answer: B
Section: (none)
Explanation

QUESTION 165

Which of the following BEST prevents collusion?

A. Separation of duties
B. Signal sign-on
C. Mandatory vacations
D. Job rotation

Correct Answer: C
Section: (none)
Explanation

QUESTION 166
Which of the following allows Pete, a security technician, to recover from a loss of staff after an earthquake?

A. Business continuity plan
B. Continuity of operations
C. Disaster recovery
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

QUESTION 167
Jane, an administrator, values transport security strength above network speed when implementing an SSL VPN. Which of the following encryption ciphers would BEST meet her needs?

A. SHA256
B. RC4
C. 3DES
D. AES128

Correct Answer: D
Section: (none)
Explanation

QUESTION 168
Which of the following is an authentication method that can be secured by using SSL?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 169

Which of the following is a symmetrical key block cipher that encrypts MOST quickly?

A. 3DES
B. RSA
C. Blowfish
D. SHA256
E. Diffie-Hellman

Correct Answer: C
Section: (none)
Explanation

QUESTION 170
Which of the following would BEST meet a server authentication requirement for a wireless network, but the network has no PKI in place?

A. PEAP
B. PAP
C. EAP-TLS
D. LEAP

Correct Answer: D
Section: (none)
Explanation

QUESTION 171
Which of the following can be used to determine which services may be running on a host, but not if they are exploitable?

A. Baseline analyzer
B. Port scanner
C. Virus scanner
D. Vulnerability scanner

Correct Answer: B
Section: (none)
Explanation

QUESTION 172
Which of the following, when incorporated into a disk encryption solution, adds the MOST security?

A. SHA256 hashing
B. Password complexity requirement
C. HMAC
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

QUESTION 173
Upon inspecting sniffer traffic, Jane, a technician, observes an entry that originates from port TCP 53422 with a destination of TCP 22. Which of the following protocols is MOST likely in use?

A. HTTP
B. HTTPS
"First Test, First Pass" - www.lead2pass.com 43
CompTIA SY0-301 Exam
C. SSH
D. DNS

Correct Answer: C
Section: (none)
Explanation

QUESTION 174
Role-based access control is BEST defined as an authorization system by which:

A. Privileges are granted to persons based on membership in one or more functional groups.
B. A separate user account is created for each functional role a person has.
C. Access is limited to the time of day a person is expected to work.
D. Privileges are assigned to each person based upon authorized requests.

Correct Answer: A
Section: (none)
Explanation

QUESTION 175
Which of the following fire suppression systems should be used in a datacenter that will put out the fire and not cause physical harm to equipment and data?

A. Water
B. Halon
C. Oxygen
D. Foam

Correct Answer: B
Section: (none)
Explanation

QUESTION 176
In order to enter a corporate office, employees must enter a PIN. Which of the following are common risks when using this type of entry system? (Select TWO)

A. Shoulder surfing
B. Key logging
C. Tailgating
D. Man-in-the-middle attacks
E. Dumpster diving

Correct Answer: AC
Section: (none)

Explanation

QUESTION 177
Which of the following is often used to verify connectivity on a network?

A. DNS
B. DHCP
C. ICMP
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 44
CompTIA SY0-301 Exam

QUESTION 178
Which of the following is BEST identified as an attack where a large number of users are fooled into entering user credentials into a fake website?

A. Pharming
B. Whaling
C. Phishing
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

QUESTION 179
Sara, a student, is interested in learning about distributed denial of service attacks. Which of the following types of malware is MOST likely the primary focus of her study?

A. Botnets
B. Logic bombs
C. Spyware
D. Trojans

Correct Answer: A
Section: (none)
Explanation

QUESTION 180
Which of the following BEST describes a DMZ?

A. A subnet that allows all outbound activity
B. A network that allows all inbound traffic
C. A transitional subnet that screens all traffic
D. A subnet that denies all inbound connectivity

Correct Answer: C
Section: (none)
Explanation

QUESTION 181
Following the order of volatility, taking hashes, and maintaining a chain of custody describes which of the following?

A. Forensics
B. Incident response
C. Business continuity
D. Disaster recovery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
New Questions

QUESTION 182
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

QUESTION 183
Sara and Jane, users, are reporting an increase in the amount of unwanted email that they are receiving each day. Which of the following would be the BEST way to respond to this issue without creating a lot of administrative overhead?

A. Deploy an anti-spam device to protect the network.
B. Update the anti-virus definitions and make sure that it is set to scan all received email
C. Set up spam filtering rules in each user's mail client.
D. Change the firewall settings to block SMTP relays so that the spam cannot get in.

Correct Answer: A
Section: (none)
Explanation

QUESTION 184
Which of the following is similar to a smurf attack, but uses UDP instead to ICMP?

A. X-Mas attack

B. Fraggle attack
C. Vishing
D. Man-in-the-middle attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 185
Pete, a security administrator, wants to secure remote telnet services and decides to use the services over SSH. Which of the following ports should Pete allow on the firewall by default?

A. 21
B. 22
C. 23
D. 25

Correct Answer: B
Section: (none)
Explanation

QUESTION 186
Which of the following accurately describes the STRONGEST multifactor authentication?

A. Something you are, something you have
B. Something you have, something you know
C. Something you are near to, something you have
D. Something you have, someone you know

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 46
CompTIA SY0-301 Exam

QUESTION 187
Which of the following is the BEST solution to securely administer remote servers?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 188
A company has sent all of its private keys to a third party. The third party company has created a secure list of these keys. Which of the following has just been implemented?

A. Key escrow
B. CRL
C. CA
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

QUESTION 189
Which of the following authentication protocols forces centralized wireless authentication?

A. WPA2-Personal
B. WPA2-Enterprise
C. WPA2-CCMP
D. WPA2-TKIP

Correct Answer: B
Section: (none)
Explanation

QUESTION 190
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

QUESTION 191
Which of the following risks could IT management be mitigating by removing an all-in-one device?

A. Continuity of operations
B. Input validation
C. Single point of failure
D. Single sign on
"First Test, First Pass" - www.lead2pass.com 47
CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

QUESTION 192
Social networking sites are used daily by the marketing team for promotional purposes. However, confidential company information, including product pictures and potential partnerships, have been inadvertently exposed to

the public by dozens of employees using social networking sites. Which of following is the BEST response to mitigate this threat with minimal company disruption?

A. Mandate additional security awareness training for all employees.
B. Report each employee to Human Resources for termination for violation of security policies
C. Implement a data loss prevention program to filter email.
D. Block access to social networking sites from the corporate network

Correct Answer: A
Section: (none)
Explanation

QUESTION 193
A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date. Which of the following BEST describes this system type?

A. NAT
B. NIPS
C. NAC
D. DMZ

Correct Answer: C
Section: (none)
Explanation

QUESTION 194
Sara, an IT administrator, wants to protect a cluster of servers in a DMZ from zero day attacks. Which of the following would provide the BEST level of protection?

A. NIPS
B. NIDS
C. ACL
D. Antivirus

Correct Answer: A
Section: (none)
Explanation

QUESTION 195
Which of the following inspects traffic entering or leaving a network to look for anomalies against expected baselines?

A. IPS
B. Sniffers
C. Stateful firewall
D. Stateless firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which of the following BEST describes a software vulnerability that is actively being used by Sara and Jane, attackers, before the vendor releases a protective patch or update?

A. Buffer overflow
B. IV attack
C. Zero day attack
D. LDAP injection

Correct Answer: C
Section: (none)
Explanation

QUESTION 197
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

QUESTION 198
Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

A. Phishing
B. Shoulder surfing
C. Impersonation
D. Tailgating

Correct Answer: C
Section: (none)
Explanation

QUESTION 199
Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

A. IV attack
B. Interference
C. Blue jacking
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

QUESTION 200
Which of the following would Pete, a security administrator, change to limit how far a wireless

signal will travel?

A. SSID
B. Encryption methods
C. Power levels
D. Antenna placement

Correct Answer: C
Section: (none)
Explanation

Exam B

QUESTION 1
Which of the following ports should be open in order for Sara and Pete, users, to identify websites by domain name?

A. TCP 21
B. UDP22
C. TCP 23
D. UDP 53

Correct Answer: D
Section: (none)
Explanation

QUESTION 2
Sara, an administrator, suspects a denial of service attack on the network, but does not know where the network traffic is coming from or what type of traffic it is. Which of the following would help Sara further assess the situation?

A. Protocol analyzer
B. Penetration testing
C. HTTP interceptor
D. Port scanner

Correct Answer: A
Section: (none)
Explanation

QUESTION 3
Sara, a security administrator, has configured a trusted OS implementation on her servers. Which of the following controls are enacted by the trusted OS implementation?

A. Mandatory Access Controls
B. Time-based Access Controls
C. Discretionary Access Controls
D. Role Based Access Controls

Correct Answer: A
Section: (none)
Explanation

QUESTION 4
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

QUESTION 5
Pete, the security administrator, is implementing a web content fitter. Which of the following is the MOST important design consideration in regards to availability?

A. The number of filter categories
B. Other companies who are using the system
C. Fail state of the system
D. The algorithm of the filtering engine

Correct Answer: C
Section: (none)
Explanation

QUESTION 6
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

QUESTION 7
When used alone, which of the following controls mitigates the risk of Sara, an attacker, launching an online brute force password attack?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 8
Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

A. The system is running 802.1 x
B. The system is using NAC
C. The system is in active-standby mode

D. The system is virtualized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 51
CompTIA SY0-301 Exam

QUESTION 9
Which of the following security concepts establishes procedures where creation and approval are performed through distinct functions?

A. Discretionary access control
B. Job rotation
C. Separation of duties
D. Principle of least privilege

Correct Answer: C
Section: (none)
Explanation

QUESTION 10
While traveling Matt, an employee, decides he would like to download some new movies onto his corporate laptop. While installing software designed to download movies from multiple computers across the Internet. Matt agrees to share portions of his hard drive. This scenario describes one of the threats involved in which of the following technologies?

A. Social networking
B. ALE
C. Cloud computing
D. P2P

Correct Answer: D
Section: (none)
Explanation

QUESTION 11
Which of the following is an attack where Pete spreads USB thumb drives throughout a bank's parking lot in order to have malware installed on the banking systems?

A. Tailgating
B. Replay attack
C. Virus
D. Social engineering

Correct Answer: D
Section: (none)
Explanation

QUESTION 12
Pete, a security administrator, has configured and implemented an additional public intermediate CA. Which of

the following must Pete submit to the major web browser vendors in order for the certificates, signed by this intermediate, to be trusted?

A. Die root CA's private key
B. The root CA's public key
C. The intermediate CA's public key
D. The intermediate CA's private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 52
CompTIA SY0-301 Exam

QUESTION 13
Which of the following is BEST described by a scenario where organizational management chooses to implement an internal Incident Response Structure for the business?

A. Deterrence
B. Separation of duties
C. Transference
D. Mitigation

Correct Answer: D
Section: (none)
Explanation

QUESTION 14
A data loss prevention strategy would MOST likely incorporate which of the following to reduce the risk associated with data loss?

A. Enforced privacy policy, encryption of VPN connections, and monitoring of communications entering the organization.
B. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications leaving the organization.
C. Enforced privacy policy, encryption of VPN connections, and monitoring of communications leaving the organization.
D. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications entering the organization.

Correct Answer: B
Section: (none)
Explanation

QUESTION 15
In a wireless network, which of the following components could cause too much coverage, too little coverage, and interference?

A. MAC filter
B. AP power levels
C. Phones or microwaves

D. SSID broadcasts

Correct Answer: B
Section: (none)
Explanation

QUESTION 16
Which of the following has a default port of 22?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 17
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: CEF
Section: (none)
Explanation

QUESTION 18
Pete, a network administrator, implements the spanning tree protocol on network switches. Which of the following issues does this address?

A. Flood guard protection
B. ARP poisoning protection
C. Loop protection
D. Trunking protection

Correct Answer: C
Section: (none)
Explanation

QUESTION 19
Matt, a security administrator, has noticed that the website and external systems have been subject to many attack attempts. To verify integrity of the website and critical files, Matt should:

A. Require all visitors to the public web home page to create a username and password to view the pages in the website
B. Configure the web application firewall to send a reset packet to the incoming IP from where an attack or scan signature has been detected.
C. Create file hashes for website and critical system files, and compare the current file hashes to the baseline at regular time intervals.
D. Reboot the web server and database server nightly after the backup has been completed.

Correct Answer: C
Section: (none)
Explanation

QUESTION 20
Matt, the administrator, has been told to confirm what account an email was sent from. Which of the following is this an example of?

A. Surveillance
B. E-discovery
C. Chain of custody
D. Integrity

Correct Answer: B
Section: (none)
Explanation

QUESTION 21
Which of the following could physically damage a device if a long term failure occurred?

A. OVAL
B. HVAC
C. Battery backup system
D. Shielding

Correct Answer: B
Section: (none)
Explanation

QUESTION 22
An administrator in a small office environment has implemented an IDS on the network perimeter to detect malicious traffic patterns. The administrator still has a concern about traffic inside the network originating between client workstations. Which of the following could be implemented?

A. HIDS
B. A VLAN
C. A network router
D. An access list

Correct Answer: A

Section: (none)
Explanation

QUESTION 23
Which of the following is the MOST important reason to verify the integrity of acquired data in a forensic investigation?

A. To ensure that a virus cannot get copied to the target media
B. To ensure that the MBR gets transferred successfully to the target media
C. To ensure that source data will fit on the specified target media
D. To ensure that the data has not been tampered with

Correct Answer: D
Section: (none)
Explanation

QUESTION 24
When should a technician perform penetration testing?

A. When the technician suspects that weak passwords exist on the network
B. When the technician is trying to guess passwords on a network
C. When the technician has permission from the owner of the network
D. When the technician is war driving and trying to gain access

Correct Answer: C
Section: (none)
Explanation

QUESTION 25
Installing an application on every desktop in a companys network that watches for possible intrusions would be an example of:

A. a HIDS.
B. a personal software firewall.
C. hardening.
D. a NIDS.

Correct Answer: A
Section: (none)
Explanation

QUESTION 26
Which of the following is the main difference between a substitution cipher and a transposition cipher when used to encode messages?

A. One rearranges and replaces blocks while the other rearranges only.
B. One replaces blocks with other blocks while the other rearranges only.
C. One replaces blocks while the other rearranges and replaces only.
D. One is a symmetric block cipher and the other is asymmetric.

Correct Answer: B
Section: (none)
Explanation

QUESTION 27
All of the following are limitations of a vulnerability scanner EXCEPT:

A. it only uncovers vulnerabilities for active systems.
B. it generates a high false-positive error rate.
C. it relies on a repository of signatures.
D. it generates less network traffic than port scanning.

Correct Answer: D
Section: (none)
Explanation

QUESTION 28
A company runs a site which has a search option available to the general public. The network administrator is reviewing the site logs one day and notices an IP address filling out a specific form on the site at a rate of two submissions per second. Which of the following is the BEST option to stop this type of abuse?

A. Add a CAPTCHA feature.
B. Block the IP address.
C. Disable ActiveX.
D. Slow down the server response times.

Correct Answer: A
Section: (none)
Explanation

QUESTION 29
An administrator is worried about an attacker using a compromised user account to gain administrator access to a system. Which of the following is this an example of?

A. Man-in-the-middle attack
B. Protocol analysis
C. Privilege escalation
D. Cross-site scripting

Correct Answer: C
Section: (none)
Explanation

QUESTION 30
"First Test, First Pass" - www.lead2pass.com 56
CompTIA SY0-301 Exam

All PCs in a network share a single administrator ID and password. When the administrator attempts to remotely control a users PC the attempt fails. Which of the following should the administrator check FIRST?

A. The antivirus settings on the local PC

B. The antivirus settings on the remote PC
C. The HIPS on the remote PC
D. The HIPS on the local PC

Correct Answer: C
Section: (none)
Explanation

QUESTION 31
Which of the following is the MOST secure protocol for Pete, an administrator, to use for managing network devices?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 32
Which of the following is the BEST incident response procedure to take when a previous employee enters a facility?

A. Notify Computer Emergency Response Team (CERT) of the security breach to document it.
B. Take screenshots of the employee's workstation.
C. Take hashes of the employee's workstation.
D. Notify security to identify employee's whereabouts.

Correct Answer: D
Section: (none)
Explanation

QUESTION 33
Which of the following activities should be completed in order to detect anomalies on a network?

A. Incident management
B. Change management
C. User permissions reviews
D. Log reviews

Correct Answer: D
Section: (none)
Explanation

QUESTION 34
Which of the following reduces the likelihood of a single point of failure when a server fails?

A. Clustering
B. Virtualization

C. RAID
"First Test, First Pass" - www.lead2pass.com 57
CompTIA SY0-301 Exam
D. Cold site

Correct Answer: A
Section: (none)
Explanation

QUESTION 35
Jane, a security administrator, wants to prevent users in sales from accessing their servers after 6:00 p.m., and prevent them from accessing accounting's network at all times. Which of the following should Jane implement to accomplish these goals? (Select TWO).

A. Separation of duties
B. Time of day restrictions
C. Access control lists
D. Mandatory access control
E. Single sign-on

Correct Answer: BC
Section: (none)
Explanation

QUESTION 36
Which of the following describes the ability for a third party to verify the sender or recipient of a given electronic message during authentication?

A. Entropy
B. Principle of least privilege
C. Non-repudiation
D. Code signing

Correct Answer: C
Section: (none)
Explanation

QUESTION 37
Which of the following protocols provides Pete, an administrator, with the HIGHEST level of security for device traps?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 38

Jane has a vendors server in-house for shipping and receiving. She wants to ensure that if the server goes down that the server in-house will be operational again within 24 hours. Which of the following should Jane define with the vendor?

A. Mean time between failures
B. A warm recovery site
C. Mean time to restore
D. A hot recovery site
"First Test, First Pass" - www.lead2pass.com 58
CompTIA SY0-301 Exam

Correct Answer: C
Section: (none)
Explanation

QUESTION 39
Which of the following procedures would be used to mitigate the risk of an internal developer embedding malicious code into a production system?

A. Audit management
B. Mobile device management
C. Incident management
D. Change management

Correct Answer: D
Section: (none)
Explanation

QUESTION 40
To mitigate the adverse effects of network modifications, which of the following should Matt, the security administrator, implement?

A. Change management
B. Routine auditing
C. Incident management
D. Log auditing

Correct Answer: A
Section: (none)
Explanation

QUESTION 41
Jane, a security technician, wants to implement secure wireless with authentication. Which of the following allows for wireless to be authenticated via MSCHAPv2?

A. PEAP
B. WPA2 personal
C. TKIP
D. CCMP

Correct Answer: A
Section: (none)

Explanation

QUESTION 42
Pete, a user, is having trouble dialing into the network from their house. The administrator checks the RADIUS server, the switch connected to the server, and finds that the switch lost configuration after a recent power outage. The administrator replaces the switch and is able to ping the switch, but not the RADIUS server. Which of the following is the MOST likely cause?

A. The switch needs to have QoS setup correctly.
B. Port security is not enabled on the switch.
C. VLAN mismatch is occurring.
D. The DMZ is not setup correctly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 59
CompTIA SY0-301 Exam

QUESTION 43
Which of the following would MOST likely be implemented in order to prevent employees from accessing certain websites?

A. VPN gateway
B. Router
C. Proxy server
D. Packet filtering firewall

Correct Answer: C
Section: (none)
Explanation

QUESTION 44
When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

A. Trust models
B. CRL
C. CA
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

QUESTION 45
Sara, a security analyst, suspects that a rogue web server is running on the network. Which of the following would MOST likely be used to identify the server's IP address?

A. Port scanner
B. Telnet

C. Traceroute
D. Honeypot

Correct Answer: A
Section: (none)
Explanation

QUESTION 46
Which of the following is an improved version of the LANMAN hash?

A. LM2
B. NTLM
C. SHA
D. MD5

Correct Answer: B
Section: (none)
Explanation

QUESTION 47
Which of the following will help Matt, an administrator; mitigate the risk of static electricity?

A. Lightening rods
B. EMI shielding
C. Humidity controls

D. Temperature controls

Correct Answer: C
Section: (none)
Explanation

QUESTION 48
An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday.
Which of the following attacks does this describe?

A. Zero day
B. Directory traversal
C. Logic bomb
D. Session hijacking

Correct Answer: A
Section: (none)
Explanation

QUESTION 49
A company needs to remove sensitive data from hard drives in leased computers before the computers are returned to the supplier. Which of the following is the BEST solution?

A. Re-image with a default OS
B. Physical destruction of the hard drive
C. Format drive using a different file system
D. Sanitization using appropriate software

Correct Answer: D
Section: (none)
Explanation

QUESTION 50
Which of the following techniques floods an application with data in an attempt to find vulnerabilities?

A. Header manipulation
B. Steganography
C. Input validation
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

QUESTION 51
Jane, a security administrator, has applied security labels to files and folders to manage and restrict access. Which of the following is Jane using?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 61
CompTIA SY0-301 Exam

QUESTION 52
Sara, a user, on a public Wi-Fi network logs into a webmail account and is redirected to a search engine. Which of the following attacks may be occurring?

A. Evil twin
B. Bluesnarfing
C. War chalking
D. Bluejacking

Correct Answer: A
Section: (none)
Explanation

QUESTION 53

When moving from an internally controlled environment to a fully outsourced infrastructure environment, such as cloud computing, it is MOST important to:

A. Implement mandatory access controls.
B. Ensure RAID 0 is implemented on servers.
C. Impose time of day restrictions across all services
D. Encrypt all confidential data.

Correct Answer: D
Section: (none)
Explanation

QUESTION 54
Which of the following would help Pete, an administrator, prevent access to a rogue access point connected to a switch?

A. Enable spanning tree protocol
B. Enable DHCP snooping
C. Disable VLAN trunking
D. Establish a MAC limit and age

Correct Answer: D
Section: (none)
Explanation

QUESTION 55
A company wants to have a backup site that is a good balance between cost and recovery time objectives. Which of the following is the BEST solution?

A. Hot site
B. Remote site
C. Cold site
D. Warm site

Correct Answer: D
Section: (none)
Explanation

QUESTION 56
While conducting a network audit, Sara, a security administrator, discovers that most clients are routing their network traffic through a desktop client instead of the company router. Which of the following is this attack type?

A. ARP poisoning
B. Session hijacking
C. DNS poisoning
D. Pharming attack

Correct Answer: A

Section: (none)
Explanation

QUESTION 57
Which of the following is a reason why Pete, a security administrator, would implement port security?

A. To inspect the TPC and UDP ports of incoming traffic
B. To port C++code into Java bit-code in a secure manner
C. To implement secure datacenter electronic access
D. To limit the number of endpoints connected through the same switch port

Correct Answer: D
Section: (none)
Explanation

QUESTION 58
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Correct Answer: A
Section: (none)
Explanation

QUESTION 59
Which of the following would be the BEST reason for Jane, a security administrator, to initially select individual file encryption over whole disk encryption?

A. It provides superior key redundancy for individual files.
B. The management of keys is easier to maintain for file encryption
C. It is faster to encrypt an individual file.
D. It provides protected access to all users

Correct Answer: C
Section: (none)
Explanation

QUESTION 60
Which of the following implements two factor authentication based on something you know and something you have?

A. Users shall authenticate to the system via a Kerberos enabled authentication server working with an integrated PKI only.
B. The system shall require users to authenticate to the system with a combination of a password or PIN and a smartcard

C. The system shall authenticate only authorized users by fingerprint and retina scan.
D. Users shall possess a combination of 8 digit PINs and fingerprint scanners.

Correct Answer: B
Section: (none)
Explanation

QUESTION 61
Which of the following attacks is characterized by Sara attempting to send an email from a Chief Information Officer's (CIO's) non-corporate email account to an IT staff member in order to have a password changed?

A. Spamming
B. Pharming
C. Privilege escalation
D. Impersonation

Correct Answer: D
Section: (none)
Explanation

QUESTION 62
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. Verity the proper group membership

Correct Answer: B
Section: (none)
Explanation

QUESTION 63
Sara, an attacker, calls the company's from desk and tries to gain insider information by providing specific company information to gain the attendant's trust. The front desk immediately alerts the IT department about this incident. This is an example of which of the following?

A. Shoulder surfing
B. Whaling
C. Tailgating
D. Impersonation

Correct Answer: D
Section: (none)
Explanation

QUESTION 64
While performing basic forensic analysis of a hard drive in Sara's, the security administrator, possession, which of the following should be verified during the analysis?

A. Witness statements

B. Image hashes
C. Chain of custody
D. Order of volatility

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 64
CompTIA SY0-301 Exam

QUESTION 65
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

QUESTION 66
Which of the following allows Pete, a security technician, to prevent email traffic from entering the company servers?

A. IDS
B. URL filtering
C. VPN concentrators
D. Spam filter

Correct Answer: D
Section: (none)
Explanation

QUESTION 67
Which of the following should be implemented to secure Pete's, a network administrator, day-to- day maintenance activities? (Select TWO).

A. TFTP
B. Telnet
C. TACACS+
D. FTP
E. SSH

Correct Answer: CE
Section: (none)
Explanation

QUESTION 68

When integrating source material from an open source project into a highly secure environment, which of the following precautions should prevent hidden threats?

A. Design review
B. Code review
C. Risk assessment
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

QUESTION 69
Which of the following can Sara, a security administrator, implement to ensure that encrypted files and devices can be recovered if the passphrase is lost?

A. Private key rings
B. Trust models
C. Registration
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

QUESTION 70
An administrator responsible for building and validating security configurations is a violation of which of the following security principles?

A. Least privilege
B. Job rotation
C. Separation of duties
D. Best business practices

Correct Answer: C
Section: (none)
Explanation

QUESTION 71
Sara, a network security administrator, has been tasked with setting up a guest wireless network for her corporation. The requirements for this connection state that it must have password authentication, with passwords being changed every week. Which of the following security protocols would meet this goal in the MOST secure manner?

A. WPA ?CCMP
B. WPA ?PSK
C. WPA2-CCMP
D. WPA2-PSK

Correct Answer: D
Section: (none)
Explanation

QUESTION 72
Which of the following are security relevant policies? (Select THREE)

A. Information classification policy
B. Network access policy
C. Data security standard
D. Procurement policy
E. Domain name policy
F. Auditing and monitoring policy
G. Secure login process

Correct Answer: ABF
Section: (none)
Explanation

QUESTION 73
Which of the following attacks is manifested as an embedded HTML image object or JavaScript image tag in an email?

A. Exception handling
B. Adware
C. Cross-site request forgery
D. Cross-site scripting

Correct Answer: D
Section: (none)
Explanation

QUESTION 74
Which of the following network solutions would BEST allow Jane, a security technician, to host an extranet application for her company?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 75
Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

A. Blowfish
B. DES
C. SHA256
D. HMAC

Correct Answer: A
Section: (none)
Explanation

QUESTION 76
Which of the following could Sara, an administrator, use in a workplace to remove sensitive data at rest from the premises?

A. Network sniffer
B. Personally owned devices
C. Vulnerability scanner
D. Hardware locks

Correct Answer: B
Section: (none)
Explanation

QUESTION 77
Which of the following administrative controls BEST mitigates the risk of ongoing inappropriate employee activities in sensitive areas?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 78
Traffic has stopped flowing to and from the company network after the inline IPS hardware failed.
Which of the following has occurred?

A. Failsafe
B. Congestion
C. Fuzzing
D. Disaster recovery

Correct Answer: A
Section: (none)
Explanation

QUESTION 79
A company is installing a wireless network in a building that houses several tenants. Which of the following should be considered to make sure none of the other tenants can detect the company's wireless network? (Select TOO).

A. Static IP addresses
B. Wireless encryption
C. MAC filtering
D. Antenna placement
E. Power levels

Correct Answer: DE
Section: (none)
Explanation

QUESTION 80
Pete is reporting an excessive amount of junk mail on the network email server. Which of the following would ONLY reduce the amount of unauthorized mail?

A. Network firewall
B. Port 25 restriction
C. Spam fitters
D. URL filters

Correct Answer: C
Section: (none)
Explanation

QUESTION 81
Which of the following network devices will prevent port scans?

A. Firewall
B. Load balancers
C. NIDS
D. Sniffer

Correct Answer: A
Section: (none)
Explanation

QUESTION 82

Which of the following multifactor authentication methods uses biometrics?

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

Correct Answer: D

Section: (none)
Explanation

QUESTION 83
Marketing creates a new folder and requests the following access be assigned:

Sales Department - Read
Marketing Department - Full Control
Inside Sales - Read Write

This is an example of which of the following?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 84
Sara, the software security engineer, is trying to detect issues that could lead to buffer overflows or memory leaks in the company software. Which of the following would help Sara automate this detection?

A. Input validation
B. Exception handling
C. Fuzzing
D. Code review

Correct Answer: C
Section: (none)
Explanation

QUESTION 85
Which of the following control types is video monitoring?

A. Detective
B. Management
C. Preventative
D. Access

Correct Answer: A
Section: (none)
Explanation

QUESTION 86
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

QUESTION 87
Which of the following allows a server to request a website on behalf of Jane, a user?

A. Sniffers
B. Proxies
C. Load balancers
D. Firewall

Correct Answer: B
Section: (none)
Explanation

QUESTION 88
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

QUESTION 89
Sara, a security administrator, has generated a key pair for the company web server. Which of the following should she do next to ensure all web traffic to the company web server is encrypted?

A. Install both the private and the public key on the client machine.
B. Install both the private and the public key on the web server.
C. Install the public key on the web server and the private key on the client machine.
D. Install the public key on the client machine and the private key on the web server.

Correct Answer: B
Section: (none)
Explanation

QUESTION 90
Pete, a security administrator, would like to implement laptop encryption to protect data. The Chief Executive Officer (CEO) believes this will be too costly to implement and decides the company will purchase an insurance policy instead. Which of the following is this an example of?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 91
Matt, a security administrator, needs to Telnet into a router to change some configurations. Which of the following ports would need to be open to allow Matt to change the configurations?

A. 23
B. 125
C. 143
D. 3389

Correct Answer: A
Section: (none)
Explanation

QUESTION 92
The IT Security Department has completed an internal risk assessment and discovered the use of an outdated antivirus definition file. Which of the following is the NEXT step that management should take?

A. Analyze the vulnerability results from the scan.
B. Mitigate risk and develop a maintenance plan.
C. Ignore risk and document appropriately to address at a later time.
D. Transfer risk to web application developers.

Correct Answer: B
Section: (none)
Explanation

QUESTION 93
Which of the following elements makes up the standard equation used to define risk? (Select TWO).

A. Confidence
B. Reproducibility
C. Impact
D. Likelihood
E. Exploitability

Correct Answer: CD
Section: (none)
Explanation

QUESTION 94
Matt's CRL is over six months old. Which of the following could Matt do in order to ensure he has the current information? (Select TWO).

A. Update the CRL
B. Change the trust model
C. Deploy a key escrow

D. Query the intermediate CA
E. Deploy a recovery agent
F. Deploy OCSP

Correct Answer: AF
Section: (none)
Explanation

QUESTION 95
Matt, the security administrator, notices a spike in the number of SQL injection attacks against a web server connected to a backend SQL database. Which of the following practices should be used to prevent an application from passing these attacks on to the database?

A. OS hardening
B. Application patch management
C. Error and exception handling
D. Input validation

Correct Answer: D
Section: (none)
Explanation

QUESTION 96
Jane's guest, Pete, comes to her office to meet her for lunch. She uses her encoded badge to enter, and he follows in behind her. This is an example of which of the following?

A. Tailgating
B. Least privilege
C. Whaling
D. Vishing

Correct Answer: A
Section: (none)
Explanation

QUESTION 97
A vulnerability has been found in a service that is unnecessary for the corporate environment. Which of the

following is the BEST way to mitigate this vulnerability?

A. Issue a hotfix to lower the vulnerability risk on the network
B. Issue a group policy to disable the service on the network.
C. Issue a service pack to ensure the service is current with all available patches
D. Issue a patch to ensure the service has a lower level of risk if compromised.

Correct Answer: B
Section: (none)
Explanation

QUESTION 98
Broadcast traffic is having a negative impact on network performance. Which of the following might help minimize this issue?

A. Use NAT to hide the IPs of each of the workstations.
B. Separate the network onto a number of different switches.
C. Separate the network into a number of different VLANs.
D. Route all the Unicast traffic through the proxy server.

Correct Answer: C
Section: (none)
Explanation

QUESTION 99
One of the concerns regarding portable digital music devices in a corporate environment is they:

A. can distract users during various security training exercises.
B. can also be used as a USB removable drive.
C. can be used as recorders during meetings.
D. may cause interference with wireless access points

Correct Answer: B
Section: (none)
Explanation

QUESTION 100
Which of the following describes separating encryption keys into multiple parts to store with trusted third parties?

A. Ticket granting ticket
B. Key recovery
C. Key escrow
D. Key registration

Correct Answer: C
Section: (none)
Explanation

QUESTION 101
Which of the following authentication services relies on a shared secret?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 102
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

QUESTION 103
Which of the following should Pete, a security technician, apply to a server to BEST prevent SYN attacks?

A. Loop protection

B. Flood guards
C. Port security
D. ACL

Correct Answer: B
Section: (none)
Explanation

QUESTION 104
When implementing a wireless network, which of the following will decrease the visibility of the network?

A. Decreasing the encryption strength
B. Disabling the SSID broadcast
C. Enabling WPA2 encryption
D. Enabling MAC filtering

Correct Answer: B
Section: (none)
Explanation

QUESTION 105

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

QUESTION 106
Mandatory vacation, job rotation, and separation of duties policies all enhance the overall security posture by doing which of the following?

A. Making it more convenient to review logs for malicious activity
B. Making it more difficult to hide malicious activity by insiders
C. Reducing risks associated with viruses and malware
D. Reducing risks associated with Internet attackers

Correct Answer: B
Section: (none)
Explanation

QUESTION 107
A recent policy change requires Pete, a security administrator, to implement TLS wherever possible. Which of the following can TLS secure? (Select THREE).

A. SNMP
B. HTTP
C. LDAP
D. ICMP
E. SMTP
F. IPSec

G. SSH

Correct Answer: BCE
Section: (none)
Explanation

QUESTION 108
Which of the following allows a company to correct security issues within their software?

A. Application fuzzing
B. Cross-site scripting
C. Configuration baseline
D. Patch management

Correct Answer: D
Section: (none)
Explanation

QUESTION 109
Matt, a security analyst, discovered that a commonly used website is serving up a script that redirects users to a questionable website. Which of the following solutions MOST likely prevents this from occurring?

A. Anti-malware
B. NIDS
C. Pop-up blocker
D. Anti-spam

Correct Answer: A
Section: (none)
Explanation

QUESTION 110
Matt, a network engineer, is setting up an IPSec VPN. Which network-layer key management standard and its protocol can be used to negotiate the connection?

A. AH
B. Kerberos
C. EAP
D. IKE

Correct Answer: D
Section: (none)
Explanation

QUESTION 111
Which of the following devices can Sara, an administrator, implement to detect and stop known attacks?

A. Signature-based NIDS
B. Anomaly-based NIDS
C. Signature-based NIPS
D. Anomaly-based NIPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 75
CompTIA SY0-301 Exam

QUESTION 112
Which of the following represents the WEAKEST password?

A. PaSsWoRd
B. P@sSWOr&
C. P@sSW1r&

D. PassW1rD

Correct Answer: A
Section: (none)
Explanation

QUESTION 113
Which of the following is mainly used for remote access into the network?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 114
In order to prevent users from surfing the web at work, Jane, the administrator, should block which of the following ports? (Select TWO).

A. TCP 25
B. TCP 80
C. TCP 110
D. TCP 443
E. UDP 80
F. UDP 8080

Correct Answer: BD
Section: (none)
Explanation

QUESTION 115
Matt, the IT administrator, wants to ensure that if any mobile device gets lost no data can be retrieved. Which of the following can he implement on the mobile devices to help accomplish this?

A. Cable locks
B. Strong passwords
C. Voice encryption
D. Remote sanitization

Correct Answer: D
Section: (none)
Explanation

QUESTION 116
Matt, a security administrator, wants to configure all the switches and routers in the network in order to security 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

QUESTION 117
Jane, a security administrator, recently configured the firewall for the corporate office. Some users report that they are unable to access any resources outside of the company. Which of the following is the MOST likely reason for the lack of access?

A. Jane forgot to save the configuration on the firewall
B. Jane forgot to account for the implicit deny statement
C. Jane forgot to connect the internal firewall port back to the switch
D. Jane specifically denied access for all users

Correct Answer: B
Section: (none)
Explanation

QUESTION 118
Which of the following describes common concerns when implementing IPS?

A. Legitimate traffic will be incorrectly blocked
B. False negatives will disrupt network throughput
C. Incompatibilities with existing routers will result in a DoS
D. Security alerts will be minimal until adequate traffic is collected

Correct Answer: A
Section: (none)
Explanation

QUESTION 119
Which of the following network design elements will allow Jane, a security technician, to access internal company resources without the use of a DS3, Satellite, or T1 connection?

A. CSU/DSU
B. Firewall
C. Router
D. DSL

Correct Answer: A
Section: (none)
Explanation

QUESTION 120

Which of the following utilizes the ECHO function of Internet Control Message Protocol (ICMP) to overwhelm a victim's system?

A. Logic bomb
B. Whaling
C. Man-in-the-middle
D. Smurf attack
"First Test, First Pass" - www.lead2pass.com 77
CompTIA SY0-301 Exam

Correct Answer: D
Section: (none)
Explanation

QUESTION 121
Matt, an administrator, is concerned about the wireless network being discovered by war driving. Which of the following can be done to mitigate this?

A. Enforce a policy for all users to authentic through a biometric device.
B. Disable all SSID broadcasting
C. Ensure all access points are running the latest firmware.
D. Move all access points into public access areas.

Correct Answer: B
Section: (none)
Explanation

QUESTION 122
Jane, the administrator of a small company, wishes to track people who access the secured server room, which is secured only by a simple hardware key lock. Jane does not have much of a budget or the approval to make significant construction changes. Given the limitations, which of the following can she do in the meantime?

A. Implement a sign in/out sheet with on-site security personnel
B. Install a 24/7 closed-circuit camera system
C. Install a separate hardware lock with limited keys
D. Implement a cipher key lock

Correct Answer: B
Section: (none)
Explanation

QUESTION 123
Which of the following enterprise security controls is BEST implemented by the use of a RADIUS server?

A. ACL
B. NAT
C. VLAN
D. 802.1X

Correct Answer: D
Section: (none)
Explanation

QUESTION 124
Pete, the security administrator at a financial institution, has finished downloading a new system patch and needs to verify its authenticity. Which of the following is the correct MD5 string for the file he downloaded?

A. 1a03b7fe4c67d9012gb42b4de49d9f3b
B. b42b4de49d9f3b1a03b7fe4c67d9012
C. 303b7fe4c67d9012b42b4de49d9f3b134
D. ab42b4de49d9f3b1a03b7f34c67d9012

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 78
CompTIA SY0-301 Exam

QUESTION 125
One of the advantages of Trusted Platform Modules (TPM) is:

A. it cannot be modified by a silent background process.
B. it is tied to the system's MAC address for secured tracking.
C. it cannot be used as the basis for securing other encryption methods.
D. it can be tied to the user's logon account for additional authentication

Correct Answer: A
Section: (none)
Explanation

QUESTION 126
Which of the following protocols is MOST closely linked with SSL?

A. SNMP
B. TLS
C. FTP
D. ICMP

Correct Answer: B
Section: (none)
Explanation

QUESTION 127
Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

A. Patch management
B. Application fuzzing
C. ID badge
D. Application configuration baseline

Correct Answer: B
Section: (none)

Explanation

QUESTION 128
Which of the following data center environmental controls must be property configured to prevent equipment failure from water?

A. Lighting
B. Temperature
C. Humidity
D. Halon fire suppression

Correct Answer: C
Section: (none)
Explanation

QUESTION 129
Matt, a corporate user, has volunteered to participate in a test group for full disk encryption on employees' laptops. After his laptop's hard drive has been fully encrypted, the network administrator is still able to access Matt's files across a SMB share. Which of the following is the MAIN reason why the files are still accessible to the administrator?

A. Matt must reboot his laptop before the encryption is activated.
B. Files moved by the network administrator off Matt's laptop are automatically decrypted
C. Full disk encryption only secures files when the laptop is powered off
D. The network administrator can decrypt anyone's files.

Correct Answer: C
Section: (none)
Explanation

QUESTION 130
Hashing and encryption provide for which of the following? (Select TWO)

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

Correct Answer: DF
Section: (none)
Explanation

QUESTION 131
A library provides automated pay per print copiers and printers. It is discovered that an employee has been embezzling money from the coin boxes for many years. Which of the following might have helped the library detect this earlier?

A. Improve employee auditing procedures
B. User education
C. Mandatory vacations
D. Acceptable use policy

Correct Answer: A
Section: (none)
Explanation

QUESTION 132
A security manager believes that too many services are running on a mission critical database server. Which of the following tools might a security analyst use to determine services that are running on the server, without logging into the machine?

A. OVAL
B. Port scanner
C. Protocol analyzer
D. NIDS

Correct Answer: B
Section: (none)
Explanation

QUESTION 133
The accounting department has a specialized check printer. Checks are printed by the accounting staff after receiving a check request from a manager. Which of the following groups needs access to this printer?

A. Accounting staff only

B. The CFO only
C. Managers only
D. Account staff and managers

Correct Answer: A
Section: (none)
Explanation

QUESTION 134
A company is addressing backup and recovery issues. The company is looking for a compromise between speed of backup and speed of recovery. Which of the following is the BEST recommendation?

A. Full backups every day
B. Daily differential backups
C. Full backups weekly with differential backups daily
D. Weekly differential with incremental backups daily

Correct Answer: C
Section: (none)
Explanation

QUESTION 135
A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If determining the risk, which of the following is the annual loss expectancy (ALE)?

A. $2,700
B. $4,500
C. $5,000
D. $7,290

Correct Answer: D
Section: (none)
Explanation

QUESTION 136
Which of the following methodologies is being used if a monitoring tool is able to detect unusual characteristics by comparing current results to previous results?

A. Definition-based
B. Signature-based
C. Performance-based
D. Anomaly-based

Correct Answer: D
Section: (none)
Explanation

QUESTION 137
A user must pass through a set of doors that enclose them in a specific area until properly authenticated. Which of the following terms BEST describes this scenario?

A. Hardware locks

B. Physical token system
C. Biometric access system
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

QUESTION 138
An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

A. Spyware
B. Trojan
C. Privilege escalation

D. DoS

Correct Answer: D
Section: (none)
Explanation

QUESTION 139
A flat or simple role-based access control (RBAC) embodies which of the following principles?

A. Users assigned to roles, permissions are assigned to groups, controls applied to groups and permissions acquired by controls
B. Users assigned permissions, roles assigned to groups and users acquire additional permissions by being a member of a group
C. Roles applied to groups, users assigned to groups and users acquire permissions by being a member of the group
D. Users assigned to roles, permissions are assigned to roles and users acquire permissions by being a member of the role

Correct Answer: D
Section: (none)
Explanation

QUESTION 140
A user reports that pop-up windows continuously appear on their screen with a message stating that they have a virus and offering to see a program that will remove it. The technician is skeptical because the antivirus definitions on the machine are up-to-date. Which of the following BEST describes what the user is seeing?

A. SQL injection
B. Spyware
C. Adware
D. SMTP open relay

Correct Answer: C
Section: (none)
Explanation

QUESTION 141
Sara, a user, needs to copy a file from a Linux workstation to a Linux server using the MOST secure file transfer method available. Which of the following protocols would she use?

A. SCP
B. FTP
C. SNMP
D. TFTP

Correct Answer: A
Section: (none)
Explanation

QUESTION 142
Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 143
Matt, a system administrator, notices that there have been many failed login attempts to the virtual server's management interface. Which of the following would be the BEST way for him to secure the virtual server's OS?

A. Implement QoS
B. Create an access control list
C. Isolate the management network
D. Enable SSH

Correct Answer: C
Section: (none)
Explanation

QUESTION 144
Which of the following wireless attacks MOST likely targets a smart phone?

A. War driving
B. Whaling
C. IV attack
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

QUESTION 145
Which of the following host security procedures will facilitate in the identification of Advanced Persistent Threats (APT)?

A. Remote wipe
B. Group policy implementation
C. Host software baselining
D. Antivirus

Correct Answer: C

Section: (none)
Explanation

QUESTION 146
Jane, a security technician, has been called into a meeting with the management team who has a requirement for comprehensive vetting of specialized employees as part of the hiring process. Funding and resources are not an issue since staff members are in high risk positions and have access to sensitive data. Which of the following access control types BEST meets the requirement?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 147
A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verily the backup datacenter is prepared for such a scenario?

A. Site visit to the backup data center
B. Disaster recovery plan review
C. Disaster recovery exercise
D. Restore from backup

Correct Answer: C
Section: (none)
Explanation

QUESTION 148
Pete, the security administrator, would like all users connecting to the corporate SSL VPN router to have up-to-date patches and antivirus signatures verified prior to accessing the internal network. Which of the following would MOST likely be employed as the verification process?

A. The router ACL matches VPN traffic. The NAC server verifies antivirus signatures are supported and up-to-date.
B. The NAC server processes the authentication, and then it matches patches and antivirus signatures with its local database.
C. The access control server connects to the agent on the users' client to set minimal accepted levels of patching and signatures allowed. The agent creates a token which the router can match for access.
D. The router sends queries to the access control server; the access control server handles proxy requests to third party patching and antivirus servers.

Correct Answer: D
Section: (none)
Explanation

QUESTION 149
In which of the following access control types does the operating system data classification determine who has access to certain resources?

A. Discretionary Access Control

B. Role based Access Control
C. Mandatory Access Control
D. Rule based Access Control

Correct Answer: C
Section: (none)
Explanation

QUESTION 150
Sara, a security administrator, needs to simplify the management of access to remote files and folders. Which of the following can she implement to BEST accomplish this?

A. Group based ACLs
B. Creating multiple copies of the files and folders
C. Discretionary access control
D. User based ACLs

Correct Answer: A
Section: (none)
Explanation

QUESTION 151
Matt, a security administrator, wants to implement a secure wireless network. Which of the following is the MOST secure wireless protocol?

A. WPA2
B. WPA
C. WEP
D. AES

Correct Answer: A
Section: (none)
Explanation

QUESTION 152
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

QUESTION 153

In order to justify the cost of a new security appliance, the administrator should do which of the following?

A. RIO analysis
B. Benchmarking
C. Market analysis
D. Usability testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 85
CompTIA SY0-301 Exam

QUESTION 154
Which of the following is responsible for masking the activity of an on-going attack from the administrator's operating system monitoring tools?

A. Rootkit
B. Botnet
C. Spyware
D. Trojan

Correct Answer: A
Section: (none)
Explanation

QUESTION 155
Which of the following forms of FTP uses TLS to securely send information?

A. SCP
B. FTPS
C. SFTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

QUESTION 156
Which of the following BEST allows Jane, a security administrator, to perform ongoing assessments of existing weaknesses within an enterprise?

A. Vulnerability scanning
B. NIPS
C. HIDS
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

QUESTION 157
Jane, an attacker, compromises a payroll system and replaces a commonly executed application with a modified version which appears to run as normal but also executes additional functions. Which of the following would BEST describe the slightly modified application?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 158
To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

A. Full disk encryption
B. Application isolation
C. Digital rights management
D. Data execution prevention

Correct Answer: A
Section: (none)
Explanation

QUESTION 159
Which of the following would allow Pete, a security analyst, to assess his company's proficiency with a particular security process?

A. Risk Assessment
B. Capability Maturity Model
C. Risk Calculation
D. Trusted Platform Module

Correct Answer: B
Section: (none)
Explanation

QUESTION 160
The Chief Security Officer (CSO) informs Jane, the technician, that there is a new requirement for all data repositories where data must be encrypted when not in use. The CSO wants Jane to apply this requirement to all corporate servers. Which of the following data encryption types will BEST fill this requirement?

A. Mobile device encryption
B. Full disk encryption
C. Transport encryption

D. Database encryption

Correct Answer: D
Section: (none)
Explanation

QUESTION 161
Jane, a security technician, needs to develop access controls for the network. In which of the following access control types does a user determine who has access to certain network resources?

A. Mandatory Access Control
B. Rule based Access Control
C. Role based Access Control
D. Discretionary Access Control

Correct Answer: D
Section: (none)
Explanation

QUESTION 162
Which of the following should Pete, the security technician, use to secure DNS zone transfers?

A. VLAN
B. DIMSSEC
C. ACL

D. 802.1X

Correct Answer: C
Section: (none)
Explanation

QUESTION 163
Matt, a network engineer, is implementing a VPN solution. Which of the following can Matt use to secure the user authentication session?

A. GPG
B. PGP
C. CHAP
D. RSA

Correct Answer: C
Section: (none)
Explanation

QUESTION 164
Sara, a user in the human resources department, requests a privacy screen for her monitor at work. Which of the following social engineering attack is Sara attempting to prevent?

A. Impersonation

B. Vishing
C. Shoulder surfing
D. Tailgating

Correct Answer: C
Section: (none)
Explanation

QUESTION 165
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

QUESTION 166
Which of the following security tools can Jane, a security administrator, use to deter theft?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 88
CompTIA SY0-301 Exam

QUESTION 167
Which of the following can be implemented on a laptop hard drive to help prevent unauthorized access to data?

A. Full disk encryption
B. Key escrow
C. Screen lock
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

QUESTION 168
Which of the following network devices allows Jane, a security technician, to perform malware inspection?

A. Load balancer
B. VPN concentrator
C. Firewall
D. NIPS

Correct Answer: D
Section: (none)
Explanation

QUESTION 169
Which of the following is a valid server-role in a Kerberos authentication system?

A. Token issuing system
B. Security assertion server
C. Authentication agent
D. Ticket granting server

Correct Answer: D
Section: (none)
Explanation

QUESTION 170
The accounting department needs access to network share A to maintain a number of financial reporting documents. The department also needs access to network share B in HR to view payroll documentation for cross-referencing items. Jane, an administrative assistant, needs access to view one document in network share A to gather data for management reports. Which of the following gives accounting and Jane the correct rights to these areas?

A. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access for the specific document on network share A.
B. Accounting should be given read/write access to network share A and read access to network share B. Jane should be given read access to network share A.
C. Accounting should be given full access to network share A and read access to network share B. Jane should be given read/write access for the specific document on network share A.
D. Accounting should be given full access to network share A and read access to network share B. Jane should be given read/write access to network share A.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 89
CompTIA SY0-301 Exam

QUESTION 171
Which of the following creates ciphertext by changing the placement of characters?

A. Transposition cryptography
B. Hashing
C. Elliptical cryptography
D. Digital signatures

Correct Answer: A
Section: (none)
Explanation

QUESTION 172
Which of the following malware types uses stealth techniques to conceal itself, cannot install itself without user interaction, and cannot automatically propagate?

A. Rootkit
B. Logic bomb
C. Adware
D. Virus

Correct Answer: A
Section: (none)
Explanation

QUESTION 173
When Pete, an employee, leaves a company, which of the following should be updated to ensure Pete's security access is reduced or eliminated?

A. RSA
B. CA
C. PKI
D. CRL

Correct Answer: D
Section: (none)
Explanation

QUESTION 174
Which of the following should Matt, an administrator, change FIRST when installing a new access point?

A. SSID broadcast
B. Encryption
C. DHCP addresses
D. Default password

Correct Answer: D
Section: (none)
Explanation

QUESTION 175
A datacenter has two rows of racks which are facing the same direction. Sara, a consultant, recommends the racks be faced away from each other. This is an example of which of the following environmental concepts?

A. Fire suppression

B. Raised floor implementation
C. Hot and cool aisles
D. Humidity controls implementation

Correct Answer: C
Section: (none)
Explanation

QUESTION 176
Which of the following password policies is the MOST effective against a brute force network attack?

A. Password complexity
B. Password recovery
C. 30 day password expiration
D. Account lockout

Correct Answer: D
Section: (none)
Explanation

QUESTION 177
Which of the following would BEST be used by Sara, the security administrator, to calculate the likelihood of an event occurring?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 178
Which of the following should Matt, an administrator, implement in a server room to help prevent static electricity?

A. GFI electrical outlets
B. Humidity controls
C. ESD straps
D. EMI shielding

Correct Answer: B
Section: (none)
Explanation

QUESTION 179
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

QUESTION 180
Pete, an IT security technician, has been tasked with implementing physical security controls for his company's workstations. Which of the following BEST meets this need?

A. Host-based firewalls
B. Safe
C. Cable locks
D. Remote wipe

Correct Answer: C
Section: (none)
Explanation

QUESTION 181
Which of the following creates ciphertext by replacing one set of characters for another?

A. Substitution cryptography
B. Elliptical cryptography
C. Digital signatures
D. Transposition cryptography

Correct Answer: A
Section: (none)
Explanation

QUESTION 182
Sara, the IT Manager, would like to ensure that the router and switches are only available from the network administrator's workstation. Which of the following would be the MOST cost effective solution to ensure that only the network administrator can access these devices?

A. Restrict console ports
B. Time of day restrictions
C. Implement ACLs
D. Implement an out-of-band administrative network

Correct Answer: C
Section: (none)
Explanation

QUESTION 183
A company is performing internal security audits after a recent exploitation on one of their proprietary

applications. Sara, the security auditor, is given the workstation with limited documentation regarding the application installed for the audit. Which of the following types of testing methods is this?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 92
CompTIA SY0-301 Exam

QUESTION 184
A web server sitting in a secure DMZ has antivirus and anti-malware software which updates daily. The latest security patches are applied and the server does not run any database software. A day later, the web server is compromised and defaced. Which of the following is the MOST likely type of attack?

A. Header manipulation
B. Zero day exploit
C. Session hijacking
D. SQL injection

Correct Answer: B
Section: (none)
Explanation

QUESTION 185
Which of the following protocols is MOST likely associated with network audit logging?

A. ICMP
B. FTPS
C. DNS
D. SNMP

Correct Answer: D
Section: (none)
Explanation

QUESTION 186
Pete, a security administrator, is asked to install and configure centralized software to securely manage and collect statistics from all of the company's network devices. Which of the following should the software support?

A. 802.1x
B. ICMP
C. SNMPv3
D. SNMP

Correct Answer: C
Section: (none)

Explanation

QUESTION 187
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

QUESTION 188
"First Test, First Pass" - www.lead2pass.com 93
CompTIA SY0-301 Exam

Matt, an account manager, arrives at work early in the morning and cannot log into his workstation. He calls the help desk an hour later to open a trouble ticket, but they tell him there is nothing wrong with his account. Matt tries his login once more and is granted access. Which of the following control types BEST explains this anomaly?

A. Discretionary access control
B. Time of day restrictions
C. Separation of duties
D. Single sign-on

Correct Answer: B
Section: (none)
Explanation

QUESTION 189
A targeted email attack sent to Sara, the company's Chief Executive Officer (CEO), is known as which of the following?

A. Whaling
B. Bluesnarfing
C. Vishing
D. Dumpster diving

Correct Answer: A
Section: (none)
Explanation

QUESTION 190
Which of the following network devices allows web traffic to be distributed amongst servers?

A. Web security gateway

B. Load balancers
C. NIDS
D. Routers

Correct Answer: B
Section: (none)
Explanation

QUESTION 191
Which of the following provides the LEAST availability?

A. RAID 0
B. RAID 1
C. RAID 3
D. RAID 5

Correct Answer: A
Section: (none)
Explanation

QUESTION 192
Sara, a security guard, reports that the side of the company building has been marked with spray paint. Which of the following could this be an example of?

A. Interference
B. War driving

C. War chalking
D. War dialing

Correct Answer: C
Section: (none)
Explanation

QUESTION 193
Matt, a security administrator, has the VPN tunnel application set up so that after multiple incorrect attempts, the VPN service is disabled. Which of the following deterrent techniques does this describe?

A. Intrusions detection system
B. Baseline reporting
C. Failopen
D. Failsafe

Correct Answer: D
Section: (none)
Explanation

QUESTION 194
Sara, a user, receives a call and the caller asks if Sara would be willing to answer a few marketing questions, and in return be placed in the drawing to win a trip to Hawaii. After Sara agrees, she is transferred to an

automated service which states that some personal information needs to be collected to verify her full name, birthday, address, and email to be eligible for the Hawaii trip. After providing the details Sara is then solicited for banking preferences, general purchasing preferences, and debit card details. Which of the following BEST describes this type of attack?

A. A hoax
B. Pharming
C. Smurfing
D. Vishing

Correct Answer: D
Section: (none)
Explanation

QUESTION 195
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

QUESTION 196
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

QUESTION 197
Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table?

A. Full disk
B. Individual files
C. Database
D. Removable media

Correct Answer: C

Section: (none)
Explanation

QUESTION 198
Which of the following security controls enforces user permissions based on a job role?

A. Single sign-on access
B. Group based privileges
C. Account policy enforcement
D. User assigned privileges

Correct Answer: B
Section: (none)
Explanation

QUESTION 199
A business has paper forms on hand in the event of a credit processing system failure. This is an example of which of the following?

A. Business process re-engineering
B. Disaster recovery
C. Continuity of operations
D. Enterprise resource planning

Correct Answer: C
Section: (none)
Explanation

QUESTION 200
By default, which of the following ports would Pete, an administrator, block to prevent incoming RDP connections to a Windows Server?

A. 22
B. 161
C. 3389
D. 5631

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Exam C

QUESTION 1
Which of the following encrypts the body of a packet, rather than just the password, while sending information?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 2
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

QUESTION 3
Which of the following risk related concepts BEST supports the identification of fraud?

A. Risk avoidance
B. Job rotation
C. ALE calculation
D. Clean desk policy

Correct Answer: B
Section: (none)
Explanation

QUESTION 4
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

QUESTION 5
Which of the following are restricted to 64-bit block sizes? (Select TWO).

A. PGP
B. DES
"First Test, First Pass" - www.lead2pass.com 97
CompTIA SY0-301 Exam
C. AES256
D. RSA
E. 3DES
F. AES

Correct Answer: BE
Section: (none)
Explanation

QUESTION 6
Which of the following would be implemented to create a network inside a network?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 7
Which of the following is a system designed to lure attackers away from production systems?

A. Proxy server
B. Spam filter
C. Honeypot
D. Flood guard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

Sara, a security analyst, discovers which operating systems the client devices on the network are running by only monitoring a mirror port on the router. Which of the following techniques did Sara use?

A. Active fingerprinting
B. Passive fingerprinting
C. Protocol analyzing
D. Network enumerating

Correct Answer: B
Section: (none)
Explanation

QUESTION 9
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:
"First Test, First Pass" - www.lead2pass.com 98
CompTIA SY0-301 Exam

QUESTION 10
Matt, the Chief Information Officer (CIO), wants to protect laptop users from zero day attacks. Which of the following would BEST achieve Matt's goal?

A. Host based firewall
B. Host based IDS
C. Anti-virus
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

QUESTION 11
Which of the following is often rated based on its ability to increase the time it takes to perform an attack?

A. Safe
B. Screen lock
C. Patch management
D. Visualization

Correct Answer: A
Section: (none)
Explanation

QUESTION 12
The human resources department of a company has requested full access to all network resources, including those of the financial department. Jane, the administrator, denies this, citing:

A. Conflict of interest
B. Separation of duties
C. Role authentication
D. Implicit deny

Correct Answer: B
Section: (none)
Explanation

QUESTION 13
Which of the following is a way to gain access to a protected system while another user is entering credentials?

A. Spim
B. Shoulder surfing
C. DDoS
D. Backdoor

Correct Answer: B
Section: (none)
Explanation

QUESTION 14
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

A. Packet filtering firewall
B. VPN gateway
C. Switch
D. Router

Correct Answer: B
Section: (none)
Explanation

QUESTION 15
Jane, a security administrator, needs to deploy a wireless network where the wireless encryption key is negotiated automatically. Which of the following MUST be implemented?

A. WPA2-PSK
B. 802.1n
C. MAC filtering
D. WPA enterprise

Correct Answer: D

Section: (none)
Explanation

QUESTION 16
Which of the following can be implemented on the company gateway router to prevent IP packets with a source IP of the internal company network from being routed by the external interface of the router into the company's network?

A. 802.1x
B. Flood guards
C. Access control lists
D. Loop protection

Correct Answer: C
Section: (none)
Explanation

QUESTION 17
Which of the following BEST explains the security benefit of a standardized server image?

A. All current security updates for the operating system will have already been applied.
B. Mandated security configurations have been made to the operating system.
C. Anti-virus software will be installed and current.
D. Operating system license use is easier to track.

Correct Answer: B
Section: (none)
Explanation

QUESTION 18
Jane, the security administrator for a company, needs to assign permissions for users on her network. Which of the following would allow Jane to give ONLY the appropriate permissions necessary?

A. Separation of duties
B. Job rotation
C. Privilege escalation

D. Least privilege

Correct Answer: D
Section: (none)
Explanation

QUESTION 19
Users in the marketing department are given a different level of access to files than users in the accounting department. Which of the following types of access control does this BEST describe?

A. Standard access control
B. Role based access control
C. Mandatory access control

D. Discretionary access control

Correct Answer: B
Section: (none)
Explanation

QUESTION 20
Which of the following types of data encryption would Jane, a security administrator, use if MBR and the file systems needed to be included?

A. Full disk
B. Individual files
C. Database
D. Partial disk

Correct Answer: A
Section: (none)
Explanation

QUESTION 21
Sara, an employee, enters the datacenter but does not ensure the door was fully closed afterwards. Which of the following could directly result from this situation?

A. Clean desk policy
B. Social engineering
C. Tailgating
D. Chain of custody

Correct Answer: C
Section: (none)
Explanation

QUESTION 22
Which of the following should Pete, the security administrator, change to help mitigate the risk associated with war drivers discovering the wireless network?

A. WPA encryption
B. WEP encryption
C. MAC filtering
D. AP power levels

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 101
CompTIA SY0-301 Exam

QUESTION 23
Which of the following is used to verify the identity of the sender of a signed email?

A. Public key
B. Sender's IP
C. From field
D. Private key

Correct Answer: A
Section: (none)
Explanation

QUESTION 24
Which of the following is the MOST important security requirement for mobile devices storing PII?

A. Remote data wipe
B. GPS location service
C. VPN pass-through
D. WPA2 wireless

Correct Answer: A
Section: (none)
Explanation

QUESTION 25
Which of the following is a way to confirm that all staff members know their roles and responsibilities during an IT disaster or other IT contingency event?

A. Table-top exercise
B. Hot site
C. Disaster recovery plan
D. MTTR

Correct Answer: A
Section: (none)
Explanation

QUESTION 26
The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter
B. Geographically disparate site redundant datacenter
C. Localized clustering of the datacenter
D. Cold site implementation for the datacenter

Correct Answer: B
Section: (none)
Explanation

QUESTION 27
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

QUESTION 28
Which of the following will allow proper ventilation for servers in a data center?

A. Hot/cold aisles
B. Humidity controls
C. EMI shielding
D. Load balancing

Correct Answer: A
Section: (none)
Explanation

QUESTION 29
Which of the following combinations represents multifactor authentication?

A. Key and proximity badge
B. Fingerprint and proximity badge
C. Retina scan and voice analysis
D. Password and PIN

Correct Answer: B
Section: (none)
Explanation

QUESTION 30
Jane, an administrator, is primarily concerned with blocking external attackers from gaining information on remote employees by scanning their laptops. Which of the following security applications is BEST suited for this task?

A. Host IDS
B. Personal firewall
C. Anti-spam software
D. Anti-virus software

Correct Answer: B
Section: (none)
Explanation

QUESTION 31
Which of the following can Pete, the security administrator, implement to filter Internet traffic?

A. Warning banners
B. Spam filters
C. Host-based firewalls
D. Command shell restrictions

Correct Answer: C
Section: (none)
Explanation

QUESTION 32
"First Test, First Pass" - www.lead2pass.com 103
CompTIA SY0-301 Exam

Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

A. Remotely lock the device with a PIN
B. Enable GPS location and record from the camera
C. Remotely uninstall all company software
D. Remotely initiate a device wipe

Correct Answer: D
Section: (none)
Explanation

QUESTION 33
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

QUESTION 34
Matt, the security administrator, is implementing a new design to minimize the footprint in the datacenter and reduce the amount of wasted resources without losing physical control of the equipment. Which of the following would Matt need to implement?

A. Visualization
B. Cloud computing
C. New ACLs
D. VLAN management

Correct Answer: A
Section: (none)
Explanation

QUESTION 35
A third party application has the ability to maintain its own user accounts or it may use single sign- on. To use single sign-on, the application is requesting the following information: OU=Users, DC=Domain, DC=COM. This application is requesting which of the following authentication services?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 36
Which of the following can grant access based solely on TCP/IP information?

A. Time of day restrictions
"First Test, First Pass" - www.lead2pass.com 104
CompTIA SY0-301 Exam
B. Implicit deny
C. ACLs
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

QUESTION 37
Which of the following should Sara, a technician, apply to prevent guests from plugging in their laptops and accessing the company network?

A. Secure router configuration
B. Port security
C. Sniffers
D. Implicit deny

Correct Answer: B
Section: (none)
Explanation

QUESTION 38
Which of the following is based on X.500 standards?

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

Correct Answer: D
Section: (none)

Explanation

QUESTION 39
Which of the following functions of a firewall allows Pete, an administrator, to map an external service to an internal host?

A. AP isolation
B. Port forwarding
C. DMZ
D. NAT

Correct Answer: B
Section: (none)
Explanation

QUESTION 40
Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

A. Rootkit
B. Logic bomb
C. Worm
D. Botnet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 105
CompTIA SY0-301 Exam

QUESTION 41
Which of the following BEST describes hashing?

A. Encrypting the data payload and computing a unique mathematic identifier in order to detect change during transport.
B. Computing a unique mathematic identifier in order to prevent change during transport.
C. Encrypting the data payload and computing a unique mathematic identifier in order to prevent change during transport.
D. Computing a unique mathematic identifier in order to detect change during transport.

Correct Answer: D
Section: (none)
Explanation

QUESTION 42
User A is a member of the payroll security group. Each member of the group should have read/write permissions to a share. User A was trying to update a file but when the user tried to access the file the user was denied. Which of the following would explain why User A could not access the file?

A. Privilege escalation
B. Rights are not set correctly

C. Least privilege
D. Read only access

Correct Answer: B
Section: (none)
Explanation

QUESTION 43
Which of the following algorithms is faster when encrypting data?

A. Symmetric key algorithms
B. Public key algorithms
C. Whole disk encryption algorithms
D. Asymmetric key algorithms

Correct Answer: A
Section: (none)
Explanation

QUESTION 44
Which of the following BEST describes the differences between RADIUS and TACACS?

A. RADIUS encrypts client-server negotiation dialog.
B. RADIUS is a remote access authentication service.
C. TACACS encrypts client-server negotiation dialog.
D. TACACS is a remote access authentication service.

Correct Answer: C
Section: (none)
Explanation

QUESTION 45
Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation

techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Install anti-virus software on the USB drives.
C. Disable USB within the workstations BIOS.
D. Apply the concept of least privilege to USB devices.
E. Run spyware detection against all workstations.

Correct Answer: AC
Section: (none)
Explanation

QUESTION 46

Which of the following allows a technician to scan for missing patches on a device without actually attempting to exploit the security problem?

A. A vulnerability scanner
B. Security baselines
C. A port scanner
D. Group policy

Correct Answer: A
Section: (none)
Explanation

QUESTION 47
An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a:

A. stateful firewall.
B. packet-filtering firewall.
C. NIPS.
D. NAT.

Correct Answer: D
Section: (none)
Explanation

QUESTION 48
A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during non-working days. Which of the following should the technician implement to meet managements request?

A. Enforce Kerberos
B. Deploy smart cards
C. Time of day restrictions
D. Access control lists

Correct Answer: C
Section: (none)
Explanation

QUESTION 49
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. Run a last logon script to look for inactive accounts.
B. Implement an account expiration date for temporary employees.
C. Implement a password expiration policy.
D. Implement time of day restrictions for all temporary employees.

Correct Answer: B

Section: (none)
Explanation

QUESTION 50
A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of $5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If the anti-malware software is purchased, which of the following is the expected net savings?

A. $900
B. $2,290
C. $2,700
D. $5,000

Correct Answer: B
Section: (none)
Explanation

QUESTION 51
Sara, a security administrator, suspects that a web server may be under attack. The web logs have several entries containing variations of the following entries:

'or 1=1--
or1'=1--
'or1=1'--

Which of the following attacks is MOST likely occurring?

A. Zero day exploit
B. Buffer overflow
C. SQL injection
D. Man-in-the-middle

Correct Answer: C
Section: (none)
Explanation

QUESTION 52
Which of the following attacks would be used if Sara, a user, is receiving unwanted text messages?

A. Packet sniffing
B. Bluesnarfing
C. Smurf attack
D. Blue jacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 108

QUESTION 53
Which of the following practices reduces the attack surface of a wireless network? (Select TWO)

A. Antenna placement
B. Using TKIP instead on AES
C. Power-level control
D. Using WPA2 instead of WPA
E. Using RADIUS

Correct Answer: AC
Section: (none)
Explanation

QUESTION 54
Matt, a security administrator, is responsible for provisioning role-based user accounts in an enterprise environment. A user has a temporary business need to perform multiple roles within the organization. Which of the following is the BEST solution to allow the user to perform multiple roles?

A. Create expiring unique user IDs per role
B. Allow access to an existing user ID
C. Assign multiple roles to the existing user ID
D. Create an additional expiring generic user ID

Correct Answer: C
Section: (none)
Explanation

QUESTION 55
An application programmer reports to Sara, the security administrator, that the antivirus software installed on a server is interfering with one of the production HR applications, and requests that antivirus be temporarily turned off. How should Sara respond to this request?

A. Ask the programmer to replicate the problem in a test environment.
B. Turn off antivirus, but install a host intrusion prevention system on the server.
C. Update the server's antivirus and anti-malware definitions from the vendor's site
D. Turn off antivirus, but turn on the host-based firewall with a deny-all rule set.

Correct Answer: A
Section: (none)
Explanation

QUESTION 56
A packet filtering firewall can protect from which of the following?

A. SOL injection
B. Brute force attack
C. Port scan
D. DNS poisoning

Correct Answer: C

Section: (none)
Explanation

QUESTION 57
"First Test, First Pass" - www.lead2pass.com 109
CompTIA SY0-301 Exam

Which of the following can Matt, an administrator, use to ensure the confidentiality of a file when it is being sent over FTP?

A. WPA2
B. PGP
C. MD5
D. NTLMv2

Correct Answer: B
Section: (none)
Explanation

QUESTION 58
Pete, a user, submitted a form on the Internet but received an unexpected response shown below

Server Error in "/" Application
Runtime error in script on asp.net version 2.0

Which of the following controls should be put in place to prevent Pete from learning this information about the web server in the future?

A. Patch management
B. Error handling
C. Fuzzing
D. Input validation

Correct Answer: B
Section: (none)
Explanation

QUESTION 59
Employees are reporting that they are receiving unusual calls from the help desk for the purpose of verifying their user credentials. Which of the following attack types is occurring?

A. Vishing
B. Spear phishing
C. Phishing
D. Pharming

Correct Answer: A
Section: (none)
Explanation

QUESTION 60
Sara, a forensic invest gator, believes that the system image she was presented with is not the same as the

original source. Which of the following should be done to verify whether or not the image has been tampered with?

A. Compare file sizes from the original with the system image.
B. Reimage the original source with a read-only tool set to ignore errors.
C. Compare hashes of the original source and system image.
D. Compare time stamps from the original with the system image.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 110
CompTIA SY0-301 Exam

QUESTION 61
Which of the following is a feature of Kerberos?

A. One-way encryption
B. Vendor patch management
C. Only available for Linux systems
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

QUESTION 62
An SQL injection vulnerability can be caused by which of the following?

A. Password complexity
B. Improper input validation
C. Discretionary access controls
D. Cross-site request forgery

Correct Answer: B
Section: (none)
Explanation

QUESTION 63
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

QUESTION 64
Which of the following would Sara, a security administrator, utilize to identity a weakness within various applications without exploiting that weakness?

A. Protocol analyzer
B. Port scanner
C. Vulnerability scan
D. Penetration test

Correct Answer: C
Section: (none)
Explanation

QUESTION 65
Matt, a security administrator, wants to allow content owners to determine who has access to tiles. Which of the following access control types does this describe?

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

D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

QUESTION 66
Which of the following commands can Matt, an administrator, use to create a forensically sound hard drive image?

A. grep
B. dump
C. dcfldd
D. hex

Correct Answer: C
Section: (none)
Explanation

QUESTION 67
Which of the following technologies would allow the removal of a single point of failure?

A. Dual-homing a server
B. Clustering a SQL server
C. Adding a second VLAN to a switch
D. Assigning a second IP address to a NIC

Correct Answer: B
Section: (none)

Explanation

QUESTION 68
Jane, the administrator, is tasked with deploying a strong encryption cipher. Which of the following ciphers would she be the LEAST likely to choose?

A. DES
B. Two fish
C. 3DES
D. AES

Correct Answer: A
Section: (none)
Explanation

QUESTION 69
Jane, a security administrator, has completed the imaging process for 20 computers that were deployed. The image contains the operating system and all required software. Which of the following is this an example of?

A. Implementing configuration hardening
B. Implementing configuration baseline
C. Implementing due diligence
D. Deploying and using a trusted OS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 112
CompTIA SY0-301 Exam

QUESTION 70
Which of the following open standards should Pete, a security administrator, select for remote authentication of users?

A. TACACS
B. RADIUS
C. WPA2
D. RIPEMD

Correct Answer: B
Section: (none)
Explanation

QUESTION 71
Matt, a system administrator, wants to establish a nightly available SQL database. Which of the following would be implemented to eliminate a single point of failure in storage and servers?

A. RAID 5 and a storage area network
B. Two striped drives and clustering
C. Two mirrored drives and clustering

D. RAID 0 and load balancing

Correct Answer: A
Section: (none)
Explanation

QUESTION 72
Which of the following malware types is MOST commonly associated with command and control?

A. Rootkits
B. Logic bombs
C. Botnets
D. Backdoors

Correct Answer: C
Section: (none)
Explanation

QUESTION 73
Which of the following security chips does BitLocker utilize?

A. BIOS
B. CPU
C. CMOS
D. TPM

Correct Answer: D
Section: (none)
Explanation

QUESTION 74
Which of the following will require exceptions when considering the use of 802.1x port security?

A. Switches
B. Printers
C. Laptops
D. Desktops

Correct Answer: B
Section: (none)
Explanation

QUESTION 75
Which of the following data encryption types will BEST protect data in motion and at rest to a cloud provider?

A. File encryption
B. Transport
C. PKI
D. SHA-256

Correct Answer: A
Section: (none)
Explanation

QUESTION 76
Which of the following will mitigate the effects of devices in close proximity?

A. EMI shielding
B. Load balancing
C. Grounding
D. Video monitoring

Correct Answer: A
Section: (none)
Explanation

QUESTION 77
A major CA has been compromised and a new patch has been released to make necessary changes on user machines. Which of the following is likely to be updated as a part of this patch?

A. Recovery agent
B. CRL
C. Key escrow
D. PKI

Correct Answer: B
Section: (none)
Explanation

QUESTION 78
Which of the following uses both a public and private key?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 79
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

QUESTION 80
Symmetric encryption utilizes_____. While asymmetric encryption utilizes_____.

A. Public keys, one time
B. Shared keys, private keys
C. Private keys, session keys
D. Private keys, public keys

Correct Answer: B
Section: (none)
Explanation

QUESTION 81
Jane, an administrator, notices that after 2.000 attempts a malicious user was able to compromise an employee's password. Which of the following security controls BEST mitigates this type of external attack? (Select TWO).

A. Account expiration
B. IDS
C. Password complexity
D. Server logging
E. Account lockout
F. Proxy server

Correct Answer: CE
Section: (none)
Explanation

QUESTION 82
Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

A. Virtual switch
B. NAT
C. System partitioning
D. Access-list
E. Disable spanning tree
F. VLAN

Correct Answer: AF
Section: (none)
Explanation

QUESTION 83
Sara, an IT manager, wants to change the firewall rules to allow RemoteOfficeB to connect to the corporate network using SSH. Which of the following rules would only allow necessary access?

A. Permit RemoteOfficeB any port 69
B. Permit RemoteOfficeB any all
C. Permit RemoteOfficeB any port 22
D. Permit any corporate port 443

Correct Answer: C
Section: (none)
Explanation

QUESTION 84
Which of the following attacks is characterized by someone following a staff member who is entering a corporate facility?

A. Evil twin
B. Tailgating
C. Shoulder surfing
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

QUESTION 85
Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

A. Two factor authentication
B. Identification and authorization
C. Single sign-on
D. Single factor authentication

Correct Answer: A
Section: (none)
Explanation

QUESTION 86
Jane, a corporate user, is trying to secure her laptop from drive-by download before she leaves for a computer conference. Which of the following should be installed to keep Jane's laptop secure from these attacks?

A. Full disk encryption
B. Host based firewall
C. Antivirus system
D. Network based firewall

Correct Answer: C

Section: (none)
Explanation

QUESTION 87
Which of the following detection methods may generate an alert when Matt, an employee, accesses a server during non-business hours?

A. Signature
B. Time of Day restrictions
C. Heuristic
"First Test, First Pass" - www.lead2pass.com 116
CompTIA SY0-301 Exam
D. Behavioral

Correct Answer: D
Section: (none)
Explanation

QUESTION 88
Which of the following data is typically left unencrypted in software based full disk encryption?

A. OS registry
B. Extended partition
C. BIOS
D. MBR

Correct Answer: D
Section: (none)
Explanation

QUESTION 89
Which of the following is an authentication service that uses symmetrical keys and tickets?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 90
Which of the following application attacks is identified by use of the <SCRIPT> tag?

A. XSS
B. Buffer overflow
C. Directory traversal
D. Zero day

Correct Answer: A

Section: (none)
Explanation

QUESTION 91
Jane, a security architect, is working on setting up a secure email solution between internal employees and external customers. Which of the following would BEST meet her goal?

A. Public key infrastructure
B. Key escrow
C. Internal certificate authority
D. Certificate revocation list

Correct Answer: A
Section: (none)
Explanation

QUESTION 92
Which of the following allows multiple internal IP addresses to be mapped to one specific external IP address?

A. VLAN
B. NAT
C. NAC
D. PAT

Correct Answer: B
Section: (none)
Explanation

QUESTION 93
Which of the following would Jane, a security administrator, use to encrypt transmissions from streaming video transmissions, keeping in mind that each bit must be encrypted as it comes across the network?

A. IDEA
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: (none)
Explanation

QUESTION 94
Matt, a user, finds a flash drive in the parking lot and decides to see what is on it by using his company laptop. A few days later Matt reports his laptop is running slow and is unable to perform simple tasks. The security administrator notices several unauthorized applications have been installed. CPU usage is unusually high, and a collection of screenshots of Matt's recent activity has been transmitted over the network .This is an example of which of the following?

A. Backdoor

B. Logic bomb
C. Rootkit
D. Spyware

Correct Answer: D
Section: (none)
Explanation

QUESTION 95
Pete, the security administrator, found that several of the company's workstations are infected with a program aimed at stealing users' cookies and reporting them back to the malicious user. Which of the following attack types is the malicious user MOST likely to carry out with this information?

A. Man-in-the-middle
B. Session hijacking
C. Command injection
D. Trojan infection

Correct Answer: B
Section: (none)
Explanation

QUESTION 96
Sara, a security administrator, is implementing remote management for network infrastructure using SNMP. Which of the following statements is true about SNMP?

A. Read communities allow write permissions
B. Relays mail based on domain keys and access headers
C. SNMP communities are encrypted using PKI
D. Write communities allow both read and write permissions

Correct Answer: D
Section: (none)
Explanation

QUESTION 97
Which of the following mitigation techniques is Pete, a security administrator, MOST likely to implement after the software has been released to the public?

A. Error and exception handling
B. Fuzzing
C. Secure coding
D. Patch management

Correct Answer: D
Section: (none)
Explanation

QUESTION 98
Which of the following BEST defines risk?

A. A threat will have a larger impact than anticipated
B. Remediation of a known vulnerability is cost prohibitive
C. A degree of probability of loss
D. A user leaves a system unsecure

Correct Answer: C
Section: (none)
Explanation

QUESTION 99
Companies allowing remote access to internal systems or systems containing sensitive data should provide access using:

A. dial-up or broadband networks using passwords.
B. wireless networks using WPA encryption.
C. VPN with two factor authentication.
D. carrier based encrypted data networks

Correct Answer: C
Section: (none)
Explanation

QUESTION 100
Which of the following is the proper order for incident response?

A. Detection, preparation, containment, eradication, recovery
B. Preparation, detection, containment, eradication, recovery
C. Preparation, detection, recovery, eradication, containment
D. Detection, containment, eradication, recovery, preparation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 119
CompTIA SY0-301 Exam

QUESTION 101
Which of the following is considered the MOST secure wireless encryption measure to implement?

A. TKIP
B. CCMP
C. WPA2
D. WEP

Correct Answer: C
Section: (none)
Explanation

QUESTION 102
Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

A. 3DES
B. Blowfish
C. Serpent
D. AES256

Correct Answer: B
Section: (none)
Explanation

QUESTION 103
A team is developing a new application with many different screens that users can access. The team decides to simplify access by creating just two internal application roles. One role is granted read-only access to the summary screen. The other role is granted update access to all screens. This simplified access model may have a negative security impact on which of the following?

A. Remote access
B. Identity management
C. Least privilege
D. Authentication

Correct Answer: C
Section: (none)
Explanation

QUESTION 104
Which of the following would be the BEST choice for attacking a complex password hash?

A. Man in the middle
B. Dictionary files
C. Rainbow tables
D. Brute-force intrusion

Correct Answer: C
Section: (none)
Explanation

QUESTION 105
In order for Pete, a user, to logon to his desktop computer, he must provide his username, password, and use a common access card with a PIN. Which of the following authentication

methods is Pete using?

A. Single factor
B. Two factor

C. Three factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

QUESTION 106
Implementation of routine file hash validation is an example of which of the following security concepts?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 107
Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

A. Folder encryption
B. File encryption
C. Whole disk encryption
D. Steganography

Correct Answer: C
Section: (none)
Explanation

QUESTION 108
A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing
B. Mantrap
C. A guard
D. Video surveillance

Correct Answer: B
Section: (none)
Explanation

QUESTION 109
Which of the following provides authentication, authorization, and accounting services?

A. PKI
B. WPA2
C. NTLMv2

D. RADIUS

Correct Answer: D
Section: (none)
Explanation

QUESTION 110
Which of the following should be considered when implementing WPA vs. WPA2?

A. LEAP vs. PEAP
B. SSID vs. MAC
C. SHA1 vs. MD5
D. CCMP vs. TKIP

Correct Answer: D
Section: (none)
Explanation

QUESTION 111
A popular software application is used on all company workstation desktop and laptop computers. Which of the following is the BEST patch management process?

A. The patch management software should be approved by the change management group to ensure adherence to corporate policies.
B. The Chief Information Officer should approve and centrally deploy the patch to all company workstations in a staggered manner.
C. Users should individually download and verify the patch with an MD5 checksum utility before applying it to their own workstation.
D. The support team should receive vendor update notifications and deploy patches in test environment before deploying to workstations.

Correct Answer: D
Section: (none)
Explanation

QUESTION 112
Which of the following network protocols transmits a user's credentials in clear-text? (Select TWO).

A. SSH
B. HTTPS
C. SCP
D. Telnet
E. FTP
F. TFTP

Correct Answer: BE
Section: (none)
Explanation

QUESTION 113
Data classification and labeling is an example of:

A. Preventative administrative control
B. Deterrent technical control
C. Preventative technical control
D. Deterrent administrative control
"First Test, First Pass" - www.lead2pass.com 122
CompTIA SY0-301 Exam

Correct Answer: A
Section: (none)
Explanation

QUESTION 114
Jane, a security administrator, must be able to identify and validate every use of local administrative accounts across a large number of Windows and Linux servers. Which of the following offers the BEST solution?

A. Modify the system baseline to increase log retention and enable a host firewall
B. Monitor LDAP and Active Directory for the use of Administrative accounts
C. Add or enable a NIDS signature for administrative activity
D. Implement centralized log collection for each server and define a log review process

Correct Answer: D
Section: (none)
Explanation

QUESTION 115
Which of the following is MOST likely used to establish a secure connection between email gateways?

A. TLS
B. PGP
C. HTTPS
D. SCP

Correct Answer: A
Section: (none)
Explanation

QUESTION 116
Which of the following describes how Pete, an employee, gains access to a location by entering with a fellow co-worker and not using his own credentials?

A. Impersonation
B. Tailgating
C. Evil twin
D. Shoulder surfing

Correct Answer: B
Section: (none)
Explanation

QUESTION 117
Sara, 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:
"First Test, First Pass" - www.lead2pass.com 123
CompTIA SY0-301 Exam

QUESTION 118
When employees that use certificates leave the company they should be added to which of the following?

A. PKI
B. CA
C. CRL
D. TKIP

Correct Answer: C
Section: (none)
Explanation

QUESTION 119
Which of the following should Matt, a security technician, implement to identify untrusted certificates?

A. CA
B. PKI
C. CRL
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

QUESTION 120
Jane, a security analyst, noticed an increase in malware infections on a user's system. She identified an email that requests the user change her password. This attack would BEST be described as which of the following?

A. Phishing
B. Spoofing
C. Privilege escalation
D. Shoulder surfing

Correct Answer: A

Section: (none)
Explanation

QUESTION 121
A corporate datacenter operates in a humid area near an ocean and often has hardware failures. Which of the following controls would help prevent these issues?

A. Fire suppression
B. HVAC
C. RAID
D. Cold aisles

Correct Answer: B
Section: (none)
Explanation

QUESTION 122
When Pete, a security administrator, cannot verify who provided a hard drive image, then:

A. Chain of custody is preserved

B. The image must be rehashed
C. The hash must be verified
D. Chain of custody is destroyed

Correct Answer: D
Section: (none)
Explanation

QUESTION 123
If Sara, an attacker, is attempting to determine the operating system using banner information, which of the following techniques could she be using?

A. Whois lookup
B. nslookup
C. Port scanning
D. Fingerprinting

Correct Answer: D
Section: (none)
Explanation

QUESTION 124
Pete, an administrator, is creating a new security policy and must consider many stakeholders as well as current regulations, and the company direction. For the BEST success in policy roll out, which stakeholder is the MOST important for Pete to consider?

A. End users
B. Information security team
C. Senior leadership team

D. Customers and vendors

Correct Answer: C
Section: (none)
Explanation

QUESTION 125
Which of the following is an encapsulated authentication protocol?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 126
Which of the following is a layer three protocol used for VPN connections?

A. SSH
B. ICMP
C. IPSec
D. SSL

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 125
CompTIA SY0-301 Exam

QUESTION 127
Which of the following can Matt, a security administrator, implement on a mobile device to help prevent a conversation from being picked up on another device?

A. Bluetooth
B. Screen locks
C. Strong passwords
D. Voice encryption

Correct Answer: D
Section: (none)
Explanation

QUESTION 128
When a username is checked against an access list, which of the following does it provide?

A. Identification and authentication
B. Identification and authorization

C. Authentication and authorization
D. Authentication and integrity

Correct Answer: B
Section: (none)
Explanation

QUESTION 129
A network device that protects an enterprise based only on source and destination addresses is BEST described as:

A. IDS
B. ACL
C. Stateful packet filtering
D. Simple packet filtering

Correct Answer: D
Section: (none)
Explanation

QUESTION 130
Which of the following terms is used to describe predictable failure points for equipment or services?

A. RTO
B. MTTR
C. RPO
D. MTBF

Correct Answer: D
Section: (none)
Explanation

QUESTION 131
Which of the following account policies would Sara, a security administrator, implement to disable a user's account after a certain period of time?

A. Lockout

B. Expiration
C. Complexity
D. Recovery

Correct Answer: B
Section: (none)
Explanation

QUESTION 132
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

QUESTION 133
Which of the following should Pete, an administrator, use to verify the integrity of a downloaded file?

A. CRL
B. CSR
C. AES
D. MD5

Correct Answer: D
Section: (none)
Explanation

QUESTION 134
Pete, a security analyst, must authenticate himself and his company when obtaining a certificate. Which of the following would validate this information for Pete?

A. Certification authority
B. Key escrow
C. Registration authority
D. Trust model

Correct Answer: C
Section: (none)
Explanation

QUESTION 135
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

QUESTION 136
Jane, a user, has reported an increase in email phishing attempts. Which of the following can be implemented to mitigate the attacks?

A. Anti-spyware
B. Anti-adware
C. Anti-virus
D. Anti-spam

Correct Answer: D
Section: (none)
Explanation

QUESTION 137
Which of the following is a policy that would force all users to organize their areas as well as help in reducing the risk of possible data theft?

A. Password behaviors
B. Clean desk policy
C. Data handling
D. Data disposal

Correct Answer: B
Section: (none)
Explanation

QUESTION 138
Which of the following is the BEST reason to have a formal and exercised incident management plan?

A. All vulnerabilities are mitigated
B. Users do not maintain excessive permissions
C. Patches are not made without testing
D. All parties understand their role in the process

Correct Answer: D
Section: (none)
Explanation

QUESTION 139
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:
"First Test, First Pass" - www.lead2pass.com 128

QUESTION 140
Which of the following time periods is a best practice for requiring user awareness training?

A. Every 5 years
B. Every 3 years
C. Every 2 years
D. Annually

Correct Answer: D
Section: (none)
Explanation

QUESTION 141
In which of the following locations would Sara, a forensic analyst, look to find a hooked process?

A. BIOS
B. Slack space
C. RAM
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

QUESTION 142
A company notices that there is a flaw in one of their proprietary programs that the company runs in-house. The flaw could cause damage to the HVAC system. Which of the following would the company transfer to an insurance company?

A. Risk
B. Threat
C. Vulnerability
D. Code review

Correct Answer: A
Section: (none)
Explanation

QUESTION 143
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

QUESTION 144
Which of the following, when used on a file, creates a non-reversible numeric representation of the file's composition?

A. AES
"First Test, First Pass" - www.lead2pass.com 129
CompTIA SY0-301 Exam
B. SHA
C. 3DES
D. RC4

Correct Answer: B
Section: (none)
Explanation

QUESTION 145
Banning of personally owned electronic devices at work BEST strengthens which of the following security principles?

A. Encourages hard drive encryption
B. Impedes shoulder surfing
C. Prevention of data leakage
D. Decreases workplace disruption

Correct Answer: C
Section: (none)
Explanation

QUESTION 146
Pete, the Chief Security Officer (CSO), is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

A. Create a single, shared user account for every system that is audited and logged based upon time of use.
B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
C. Enact a policy that employees must use their vacation time in a staggered schedule.
D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Correct Answer: C
Section: (none)
Explanation

QUESTION 147
Jane, a user, has attempted to enter her username and password three times unsuccessfully. Jane receives a message to try again in one hour. This is an example of which of the following?

A. Account expiration
B. Account recovery
C. Account lockout

D. Account disablement

Correct Answer: C
Section: (none)
Explanation

QUESTION 148
Sara, an attacker, tricks a user into authenticating to a fake wireless network and then inserts malicious code into strings as the user passes by. Which of the following describes this attack?

A. SQL injection
B. Malicious insider
C. Evil twin

D. User impersonation

Correct Answer: C
Section: (none)
Explanation

QUESTION 149
Which of the following is a vulnerability associated with disabling pop-up blockers?

A. An alert message from the administrator may not be visible
B. A form submitted by the user may not open
C. The help window may not be displayed
D. Another browser instance may execute malicious code

Correct Answer: D
Section: (none)
Explanation

QUESTION 150
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. Visualization
B. Remote access
C. Network access control
D. Blade servers

Correct Answer: A
Section: (none)
Explanation

QUESTION 151
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

QUESTION 152
Which of the following could be applied on a router in order to permit or deny certain ports?

A. Port security
B. Subnetting
C. Access control lists
D. Network address translation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 131
CompTIA SY0-301 Exam

QUESTION 153
Which of the following BEST describes a denial of service attack?

A. Sara, the attacker, attempts to have the receiving server run a payload using programming commonly found on web servers.
B. Sara, the attacker, overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
C. Sara, the attacker, overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.
D. Sara, the attacker, attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.

Correct Answer: B
Section: (none)
Explanation

QUESTION 154
The Chief Information Officer (CIO) wants to protect laptop users from zero day attacks. Which of the following would BEST achieve the CIO's goal?

A. Host based firewall
B. Host based IDS
C. Anti-virus
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

QUESTION 155
Matt, a server administrator, sets up database forms based on security rating levels. If a user has the lowest security rating then the database automatically determines what access that user has. Which of the following access control methods does this describe?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 156
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

QUESTION 157
Pete, a security administrator, has observed repeated attempts to break into the network. Which of

the following is designed to stop an intrusion on the network?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 158
Jane, an IT security technician working at a bank, has implemented encryption between two locations. Which of the following security concepts BEST exemplifies the protection provided by this example?

A. Integrity
B. Confidentiality
C. Cost

D. Availability

Correct Answer: B
Section: (none)
Explanation

QUESTION 159
While Sara is logging into the server from her workstation, she notices Pete watching her enter the username and password. Which of the following social engineering attacks is Pete executing?

A. Impersonation
B. Tailgating
C. Piggybacking
D. Shoulder surfing

Correct Answer: D
Section: (none)
Explanation

QUESTION 160
The log management system at Company A is inadequate to meet the standards required by their corporate governance team. A new automated log management system has been put in place.
This is an example of which of the following?

A. Data integrity measurement
B. Network traffic analysis
C. Risk acceptance process
D. Continuous monitoring

Correct Answer: D
Section: (none)
Explanation

QUESTION 161
Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

A. Trojan virus

B. Botnet
C. Worm outbreak
D. Logic bomb

Correct Answer: C
Section: (none)
Explanation

QUESTION 162
Which of the following should Sara, a security technician, perform as the FIRST step when creating a disaster recovery plan for a mission critical accounting system?

A. Implementing redundant systems
B. Removal of single points of failure
C. Succession planning
D. Business impact assessment

Correct Answer: D
Section: (none)
Explanation

QUESTION 163
Which of the following is a reason why a company might deploy data encryption?

A. To maintain the integrity of the information
B. To keep information confidential
C. To prevent data corruption
D. To prevent backup tape theft

Correct Answer: B
Section: (none)
Explanation

QUESTION 164
Which of the following would Sara, a security administrator, implement to divert and analyze attacks?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 165
In PKI, the public key is used to:

A. Decrypt the signature CRC
B. Decrypt an email message
C. Encrypt an email message
D. Encrypt the signature hash

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 134
CompTIA SY0-301 Exam

QUESTION 166
Jane, a security technician, needs to open ports on a firewall to allow for domain name resolution. Which of the following ports should Jane open? (Select TWO).

A. TCP 21
B. TCP 23
C. TCP 53
D. UDP 23
E. UDP 53

Correct Answer: CE
Section: (none)
Explanation

QUESTION 167
After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25
B. 68
C. 80
D. 443

Correct Answer: B
Section: (none)
Explanation

QUESTION 168
The health care department is storing files with names, addresses, and social security numbers on a corporate file server. Matt, the security analyst, comes across this data in an audit. Which of the following has Matt discovered?

A. Personal identifiable information
B. Data classification rules
C. Data disposal procedures
D. Data handling rules

Correct Answer: A
Section: (none)
Explanation

QUESTION 169
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

A. SHA1
B. MD2
C. MD4
D. MD5

Correct Answer: A
Section: (none)
Explanation

QUESTION 170
"First Test, First Pass" - www.lead2pass.com 135
CompTIA SY0-301 Exam

Which of the following would Jane, a security administrator, use to authenticate remote users into the network?

A. RADIUS
B. XTACACS
C. TACACS
D. ACLs

Correct Answer: A
Section: (none)
Explanation

QUESTION 171
A company wants to implement a policy that helps reduce employee stress and decrease the likelihood of security incidents caused by job dissatisfaction. Which of the following will MOST likely have a positive impact on the employee stress and job satisfaction?

A. Change management
B. Mandatory vacations
C. Due care
D. Service Level Agreements

Correct Answer: B
Section: (none)
Explanation

QUESTION 172
Pete would like to implement a new tape backup plan for HR to speed up the process of nightly backups on their file systems HR does not make many file alterations on Tuesday through Thursday. Pete does a full backup on Monday and again on Friday. Which of the following should Pete do to speed up the backups Tuesday through Thursday?

A. Incremental backups Tuesday through Thursday
B. Full backups Tuesday through Thursday
C. Differential backups Tuesday through Thursday
D. Differential backups Tuesday and Wednesday

Correct Answer: A
Section: (none)
Explanation

QUESTION 173
Hashing algorithms are used to address which of the following?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 174
After setting up a root CA. which of the following can Pete, a security administrator, implement to allow intermediate CAs to handout keys and certificates?

A. CRL
B. Spanning tree
C. Trust model
D. Key escrow

Correct Answer: C
Section: (none)
Explanation

QUESTION 175
Which of the following should be implemented to restrict wireless access to the hardware address of a NIC?

A. URL filtering
B. WPA2 and EAP
C. PEAP and WPA
D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

QUESTION 176
Which of the following is the purpose of the spanning tree protocol?

A. Loop protection
B. Access control lists
C. Secure device configuration
D. Implicit deny

Correct Answer: A
Section: (none)
Explanation

QUESTION 177
Sara, the security engineer, has discovered that a breach is in progress on a non-production system of moderate importance. Which of the following should Sara collect FIRST?

A. Memory dump, ARP cache
B. Live system image, route table
C. Temp files, hosts file

D. Offline system image, router logs

Correct Answer: A
Section: (none)
Explanation

QUESTION 178
While traveling, users need access to an internal company web server that contains proprietary information. Pete, the security administrator, should implement a:

A. NAC
B. VLAN
C. DMZ
D. RAS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 137
CompTIA SY0-301 Exam

QUESTION 179
Which of the following is used by Matt, a security administrator, to lower the risks associated with electrostatic discharge, corrosion, and thermal breakdown?

A. Temperature and humidity controls
B. Routine audits
C. Fire suppression and EMI shielding
D. Hot and cold aisles

Correct Answer: A
Section: (none)
Explanation

QUESTION 180
Workers of a small local organization have implemented an off-site location in which the organization can resume operations within 10 business days in the event of a disaster. This type of site is BEST known as which of the following?

A. Hot site
B. High-availability site
C. Cold site
D. Warm site

Correct Answer: C
Section: (none)
Explanation

QUESTION 181
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

QUESTION 182
Which of the following ports would be blocked if Pete, a security administrator, wants to disable FTP?

A. 21
B. 23
C. 25
D. 110

Correct Answer: A
Section: (none)
Explanation

QUESTION 183
Which of the following tools will allow a technician to detect security-related TCP connection anomalies?

A. Logical token
B. Performance monitor
C. Public key infrastructure
D. Trusted platform module

Correct Answer: B
Section: (none)
Explanation

QUESTION 184
An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns. Which of the following is an example of this threat?

A. An attacker using the phone remotely for spoofing other phone numbers
B. Unauthorized intrusions into the phone to access data
C. The Bluetooth enabled phone causing signal interference with the network
D. An attacker using exploits that allow the phone to be disabled

Correct Answer: B
Section: (none)
Explanation

QUESTION 185
Which of the following is the difference between identification and authentication of a user?

A. Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.
B. Identification tells who the user is and authentication proves it.
C. Identification proves who the user is and authentication is used to keep the users data secure.
D. Identification proves who the user is and authentication tells the user what they are allowed to do.

Correct Answer: B
Section: (none)
Explanation

QUESTION 186
The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

A. The risks associated with the large capacity of USB drives and their concealable nature
B. The security costs associated with securing the USB drives over time
C. The cost associated with distributing a large volume of the USB pens
D. The security risks associated with combining USB drives and cell phones on a network

Correct Answer: A
Section: (none)
Explanation

QUESTION 187
A technician is investigating intermittent switch degradation. The issue only seems to occur when the buildings roof air conditioning system runs. Which of the following would reduce the connectivity issues?

A. Adding a heat deflector
B. Redundant HVAC systems
C. Shielding
D. Add a wireless network

Correct Answer: C
Section: (none)
Explanation

QUESTION 188
According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 189
A technician is testing the security of a new database application with a website front-end. The technician notices that when certain characters are input into the application it will crash the server. Which of the following does the technician need to do?

A. Utilize SSL on the website
B. Implement an ACL
C. Lock-down the database
D. Input validation

Correct Answer: D
Section: (none)
Explanation

QUESTION 190
An organization is installing new servers into their infrastructure. A technician is responsible for making sure that all new servers meet security requirements for uptime. In which of the following is the availability requirements identified?

A. Service level agreement
B. Performance baseline
C. Device manufacturer documentation
D. Security template

Correct Answer: A
Section: (none)
Explanation

QUESTION 191
Why is bluesnarfing more of a security concern than blue jacking?

A. Data is completely erased as soon as contact has been established from another device.
B. The target device has its data accessed or stolen from another Bluetooth device.
C. The device will be rendered inoperable.

D. The target device is remotely accessed and unsolicited messages are sent.

Correct Answer: B
Section: (none)
Explanation

QUESTION 192
Which of the following is the MOST effective way to minimize restoration time and conserve storage space while adhering to industry best practices?

A. Perform full backups weekly and differential backups nightly, with the tapes stored in a secure, off-site location.
B. Perform full backups weekly and differential backups nightly, with the tapes stored in the server room for quick access.

C. Perform full backups weekly and incremental backups nightly, with the tapes stored in the server room for quick access.
D. Perform full backups weekly and incremental backups nightly, with the tapes stored in a secure, off-site location.

Correct Answer: A
Section: (none)
Explanation

QUESTION 193
A company takes orders exclusively over the Internet. Customers submit orders via a web-based application running on the external web server which is located on Network A. Warehouse employees use an internal application, on its own server, to pick and ship orders this is located on Network B. Any changes made after the order is placed are handled by a customer service representative using the same internal application. All information is stored in a database, which is also located on Network B. The company uses these three sets of user rights:
- NONE
- ADD (read existing data, write new data)
- CHANGE (read, write and change existing data)

The company has 2 different network zones:
- Network A, the DMZ, a public accessible network
- Network B, the internal LAN, accessible from company systems only

The company wants to restrict customer access as much as possible without impeding their ability to place orders. Which of the following permissions is the MOST appropriate for the customers?

A. ADD on Network A, NONE on Network B
B. CHANGE on Network A, NONE on Network B
C. CHANGE on Network A and B
D. CHANGE on Network A, ADD on Network B

Correct Answer: A
Section: (none)
Explanation

QUESTION 194
A company takes orders exclusively over the Internet. Customers submit orders via a web-based application running on the external web server which is located on Network A. Warehouse employees use an internal application, on its own server, to pick and ship orders, located on network B. Any changes made after the order is placed are handled by a customer service representative using the same internal application. All information is stored in a database, which is also located on network B. The company uses these three sets of user rights:

- NONE
- ADD (read existing data, write new data)
- CHANGE (read, write and change existing data)

The company has 2 different network zones:
- Network A, the DMZ, a public accessible network
- Network B, the internal LAN, accessible from company systems only

The company decides to add a separate database for the accounting department. The accounting staff also needs access to the internal application and its database. Which of the following options is the MOST cost-

effective and provides the best protection for the accounting database as well as the internal application?

A. Place the accounting database on Network B and the accounting employees on Network A.
B. Place the accounting database and accounting employees on Network B.
C. Place the accounting database and employees on Network A.
D. Create a third network with the same access as Network B for the accounting database and employees.

Correct Answer: B
Section: (none)
Explanation

QUESTION 195
A company takes orders exclusively over the Internet. Customers submit orders via a web-based application running on the external web server which is located on network A. Warehouse employees use an internal application, on its own server, to pick and ship orders, located on Network B. Any changes made after the order is placed are handled by a customer service representative using the same internal application. All information is stored in a database, which is also located on Network B. The company uses these three sets of user rights:
- NONE
- ADD (read existing data, write new data)
- CHANGE (read, write and change existing data)

The company has 2 different network zones:
- Network A, the DMZ, a public accessible network
- Network B, the internal LAN, accessible from company systems only

The company wants to restrict customer service representative access as much as possible without impeding their ability to place orders. Which of the following permissions is the MOST appropriate for the customer service representatives?

A. CHANGE on Network A and B
B. CHANGE on Network B, NONE on Network A
C. CHANGE on Network A, ADD on Network B
D. ADD on Network A, NONE on Network B

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 142
About Lead2pass.com

Lead2pass.com was founded in 2006. We provide latest & high quality IT Certification Training Exam Questions, Study Guides, Practice Tests. Lead the way to help you pass any IT Certification exams, 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

Our Slogan: First Test, First Pass.

Help you to pass any IT Certification exams at the first try.

You can reach us at any of the email addresses listed below.

Sales: sales@lead2pass.com

Support: support@lead2pass.com