SY0-301.v12.59

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

Vendor: CompTIA

Exam Code: SY0-301

Exam Name: CompTIA Security+ Certification Exam

Version: 12.59

Exam A

QUESTION 1
A security firm has been engaged to assess a software application. A production-like test environment, login details, production documentation and source code have been provided. Which of the following types of testing is being described?

A. White box
B. Gray box
C. Black box
D. Red teaming

Correct Answer: A
Section: (none)
Explanation

QUESTION 2
A user has forgotten their account password. Which of the following is the BEST recovery strategy?

A. Upgrade the authentication system to use biometrics instead.
B. Temporarily disable password complexity requirements.
C. Set a temporary password that expires upon first use.
D. Retrieve the user password from the credentials database.

Correct Answer: C
Section: (none)
Explanation

QUESTION 3
All of the following are valid cryptographic hash functions EXCEPT:

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 4
When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?

A. Lack of key escrow
B. Self-signed certificate
C. Weak certificate pass-phrase
D. Weak certificate cipher

Correct Answer: B
Section: (none)

Explanation

QUESTION 5
Which of the following PKI components identifies certificates that can no longer be trusted?

A. CRL
"First Test, First Pass" - www.lead2pass.com 4
CompTIA SY0-301 Exam
B. CA public key
C. Escrow
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

QUESTION 6
Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

A. 802.1x
B. DHCP
C. 802.1q
D. NIPS

Correct Answer: A
Section: (none)
Explanation

QUESTION 7
MAC filtering is a form of which of the following?

A. Virtualization
B. Network Access Control
C. Virtual Private Networking
D. Network Address Translation

Correct Answer: B
Section: (none)
Explanation

QUESTION 8
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 9
A company that purchases insurance to reduce risk is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 10
"First Test, First Pass" - www.lead2pass.com 5
CompTIA SY0-301 Exam

Which of the following is a method to prevent ad-hoc configuration mistakes?

A. Implement an auditing strategy
B. Implement an incident management strategy
C. Implement a patch management strategy
D. Implement a change management strategy

Correct Answer: D
Section: (none)
Explanation

QUESTION 11
Which of the following risks may result from improper use of social networking and P2P software?

A. Shoulder surfing
B. Denial of service
C. Information disclosure
D. Data loss prevention

Correct Answer: C
Section: (none)
Explanation

QUESTION 12
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 13
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 14
Which of the following would be used for secure remote terminal access?

A. SSH
B. TFTP
C. SCP
D. SFTP
"First Test, First Pass" - www.lead2pass.com 6
CompTIA SY0-301 Exam

Correct Answer: A
Section: (none)
Explanation

QUESTION 15
Without validating user input, an application becomes vulnerable to all of the following EXCEPT:

A. buffer overflow.
B. command injection.
C. spear phishing.
D. SQL injection.

Correct Answer: C
Section: (none)
Explanation

QUESTION 16
After verifying that the server and database are running, Jane, the administrator, is still unable to make a TCP connection to the database. Which of the following is the MOST likely cause for this?

A. The server has data execution prevention enabled
B. The server has TPM based protection enabled

C. The server has HIDS installed
D. The server is running a host-based firewall

Correct Answer: D
Section: (none)
Explanation

QUESTION 17
Which of the following is used to detect an unknown security vulnerability?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 18
Which of the following is a best practice before deploying a new desktop operating system image?

A. Install network monitoring software
B. Perform white box testing
C. Remove single points of failure
D. Verify operating system security settings

Correct Answer: D
Section: (none)
Explanation

QUESTION 19
Securing mobile devices involves which of the following checklists?

A. Key escrow, trust model, CRL
B. Cross-site scripting, XSRF, fuzzing

C. Screen lock, encryption, remote wipe
D. Black box, gray box, white box testing

Correct Answer: C
Section: (none)
Explanation

QUESTION 20
Which of the following steps should follow the deployment of a patch?

A. Antivirus and anti-malware deployment
B. Audit and verification

C. Fuzzing and exploitation
D. Error and exception handling

Correct Answer: B
Section: (none)
Explanation

QUESTION 21
Lack of internal security resources and high availability requirements are factors that may lead a company to consider:

A. patch management.
B. encryption.
C. cloud computing.
D. anti-malware sotware.

Correct Answer: C
Section: (none)
Explanation

QUESTION 22
Which of the following would be used when a higher level of security is desired for encryption key storage?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 23
Which of the following is the default port for SCP and SSH?

A. 21
B. 22
C. 404
D. 443

Correct Answer: B
Section: (none)
Explanation

QUESTION 24

Which of the following default ports does the hypertext transfer protocol use for non-secure network connections?

A. 20
B. 21
C. 80
D. 8080

Correct Answer: C
Section: (none)
Explanation

QUESTION 25
Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

A. Biometrics
B. PKI
C. Single factor authentication
D. Multifactor authentication

Correct Answer: D
Section: (none)
Explanation

QUESTION 26
Which of the following result types would Jane, a security administrator, MOST likely look for during a penetration test?

A. Inability to gain administrative access
B. Open ports
C. Ability to bypass security controls
D. Incorrect configurations

Correct Answer: C
Section: (none)
Explanation

QUESTION 27
A small business owner has asked the security consultant to suggest an inexpensive means to deter physical intrusions at their place of business. Which of the following would BEST meet their request?

A. Fake cameras
B. Proximity readers
C. Infrared cameras
D. Security guards

Correct Answer: A
Section: (none)
Explanation

QUESTION 28
Employee badges are encoded with a private encryption key and specific personal information. The encoding

is then used to provide access to the network. Which of the following describes this access control type?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 29
Which of the following devices would MOST likely have a DMZ interface?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 30
Which of the following is used to digitally sign an email?

A. Private key
B. Public key
C. Sender's IP
D. Sender's MAC address

Correct Answer: A
Section: (none)
Explanation

QUESTION 31
Pete, the company Chief Information Officer (CIO), has been receiving numerous emails from the help desk directing Pete to a link to verify credentials. Which of the following attacks is underway?

A. Replay attack
B. Pharming
C. Privilege escalation
D. Spear phishing

Correct Answer: D
Section: (none)
Explanation

QUESTION 32
Pete, a security administrator, noticed that the network analyzer is displaying packets that have all the bits in the option field turned on. Which of the following attacks is underway?

A. X-Mas
B. DDoS
C. Birthday
D. Smurf

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 10
CompTIA SY0-301 Exam

QUESTION 33
Which of the following tools would Matt, a security administrator, MOST likely use to analyze a malicious payload?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 34
Which of the following is Jane, a security administrator, MOST likely to install in order to capture and analyze zero day exploits?

A. Honeypot
B. Antivirus
C. IPS
D. IDS

Correct Answer: A
Section: (none)
Explanation

QUESTION 35
Which of the following can be implemented to detect file system variations?

A. EXT3
B. Hashing
C. Encryption
D. NIDS

Correct Answer: B
Section: (none)
Explanation

QUESTION 36
Which of the following threats is MOST likely to be mitigated by implementing cross-site scripting prevention tools?

A. Resource starvation
B. Insider threat
C. Spear phishing
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

QUESTION 37
An attacker has gained access to the corporate network and is attempting to brute force a password to gain access to the accounting system. Which of the following, if implemented, will protect the server?

A. Single sign-on
B. Password history
C. Limit logon attempts
D. Directory services

Correct Answer: C
Section: (none)
Explanation

QUESTION 38
Pete, a security administrator, wants to check user password complexity. Which of the following is the BEST tool to use?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 39
Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

A. Hashing

B. Transport encryption
C. Digital signatures
D. Steganography

Correct Answer: D
Section: (none)
Explanation

QUESTION 40
Certificates are used for: (Select TWO).

A. client authentication.
B. WEP encryption.
C. access control lists.
D. code signing.
E. password hashing.

Correct Answer: AD
Section: (none)
Explanation

QUESTION 41
When implementing SSL VPN, which of the following is the FASTEST cipher that Pete, an administrator, can use?

A. 3DES
B. AES
C. DES
D. RC4

Correct Answer: D
Section: (none)
Explanation

QUESTION 42
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 43
Which of the following is an operational control?

A. Concurrent session control
B. System security categorization
C. Contingency planning
D. Session locks

Correct Answer: C
Section: (none)
Explanation

QUESTION 44
Which of the following is a hardware based encryption device?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 45
Which of the following is the MOST important step for preserving evidence during forensic procedures?

A. Involve law enforcement
B. Chain of custody
C. Record the time of the incident
D. Report within one hour of discovery

Correct Answer: B
Section: (none)
Explanation

QUESTION 46
Employees of a company have received emails that fraudulently claim to be from the company's security department. The emails ask the employees to sign-on to an Internet website to verify passwords and personal information. This is an example of which type of attack?

A. Spam
B. Pharming
C. Man-in-the-middle
D. Vishing

Correct Answer: B
Section: (none)
Explanation

QUESTION 47
A company has implemented software to enforce full disk and removable media encryption for all computers. Which of the following threats can still expose sensitive data on these computers?

A. Spam
B. Botnet infection
C. Stolen laptop
D. Header manipulation

Correct Answer: B
Section: (none)
Explanation

QUESTION 48
Which of the following MOST interferes with network-based detection techniques?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 49
Which of the following secure coding concepts can prevent the unintentional execution of malicious code entered in place of proper commands?

A. Patch management
B. Proper exception handling
C. Code reviews
D. Input validation

Correct Answer: D
Section: (none)
Explanation

QUESTION 50
Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

A. Disable SSID broadcast
B. Install a RADIUS server
C. Enable MAC filtering
D. Lowering power levels on the AP

Correct Answer: C

Section: (none)
Explanation

QUESTION 51
A system administrator decides to use SNMPv3 on the network router in AuthPriv mode. Which of the following algorithm combinations would be valid?

A. AES-RC4
B. 3DES-MD5
C. RSA-DSA
D. SHA1-HMAC

Correct Answer: B
Section: (none)
Explanation

QUESTION 52
Which of the following are encryption algorithms that can use a 128-bit key size? (Select TWO).

A. AES
B. RC4
C. Twofish
D. DES
E. SHA2

Correct Answer: AC
Section: (none)
Explanation

QUESTION 53
Unsolicited address items and messages are discovered on a Chief Information Officer's (CIO's) smartphone. Additionally, files on an administrator's smartphone are changed or missing. Which of the following BEST describes what may have happened?

A. The CIO and the Administrator were both bluesnarfed.
B. The CIO and the Administrator were both bluejacked.
C. The CIO was bluejacked and the Administrator was bluesnarfed.
D. The CIO was bluesnarfed and the Administrator was bluejacked.

Correct Answer: C
Section: (none)
Explanation

QUESTION 54
Which of the following devices, connected to an IDS, would allow capture of the MOST traffic?

A. Switch
B. Router
C. Firewall
D. Hub

Correct Answer: D
Section: (none)
Explanation

QUESTION 55
Matt, an administrator, notices a flood fragmented packet and retransmits from an email server.

After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 56
Which of the following devices can be used to terminate remote user's established SSL or IPSec tunnels? (Select TWO).

A. NIDS
B. HIPS
C. VPN concentrator
D. Hub
E. Firewall

Correct Answer: CE
Section: (none)
Explanation

QUESTION 57
Jane, a user, brings in a laptop from home and gets certificate warnings when connecting to corporate intranet sites. These warnings do not occur when using any of the companies' workstations. Which of the following is MOST likely the issue?

A. The laptop needs to VPN to bypass the NAC.
B. The corporate intranet servers do not trust the laptop.
C. The laptop's CRL enrollment has expired.
D. The user's certificate store does not trust the CA.

Correct Answer: D
Section: (none)
Explanation

QUESTION 58
Which of the following mitigates the loss of a private key in PKI? (Select TWO).

A. Certificate reissue
B. Key rotation
C. Key escrow
D. Auto enrollment
E. Recovery agent

Correct Answer: CE
Section: (none)
Explanation

QUESTION 59
Which of the following specifications would Sara, an administrator, implement as a network access control?

A. 802.1q
B. 802.3
C. 802.11n
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

QUESTION 60
Which of the following malware types propagates automatically, does not typically hide, requires user interaction, and displays marketing ads?

A. Logic bombs
B. Rootkits
C. Spyware
D. Worms

Correct Answer: D
Section: (none)
Explanation

QUESTION 61
Which of the following malware types typically disguises itself within another piece of software, requires user interaction, and does not execute on a specific date?

A. Logic Bomb
B. Trojan
C. Worm
D. Botnet

Correct Answer: B

Section: (none)
Explanation

QUESTION 62
Which of the following is MOST commonly identified as an ARP spoofing attack where no email is sent, and flags within the TCP packet are irrelevant?

A. Xmas attack
B. Spam attack
C. Man-in-the-middle attack
D. DDoS attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 63
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

A. Whaling
B. Impersonation
C. Privilege escalation
D. Spear phishing
"First Test, First Pass" - www.lead2pass.com 17
CompTIA SY0-301 Exam

Correct Answer: A
Section: (none)
Explanation

QUESTION 64
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 65
Which of the following attacks significantly relies on staff members wanting to be helpful and supportive of each other?

A. Spoofing
B. Tailgating

C. Dumpster diving
D. Xmas attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 66
Which of the following is an attacker attempting to discover open wireless access points?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 67
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 68
Which of the following is designed to serve as a risk mitigation strategy?

A. Personally owned devices
B. Disaster recovery plan
C. Calculate proper ROI
D. Zero day exploits

Correct Answer: B
Section: (none)
Explanation

QUESTION 69
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team
B. Internal auditors
C. Incident response team
D. Software vendors

Correct Answer: C
Section: (none)
Explanation

QUESTION 70
Which process will determine maximum tolerable downtime?

A. Business Continuity Planning
B. Contingency Planning
C. Business Impact Analysis
D. Disaster Recovery Plan

Correct Answer: C
Section: (none)
Explanation

QUESTION 71
Which of the following provides the MOST protection against zero day attacks via email attachments?

A. Anti-spam
B. Anti-virus
C. Host-based firewalls
D. Patch management

Correct Answer: A
Section: (none)
Explanation

QUESTION 72
Which of the following access controls enforces permissions based on data labeling at specific levels?

A. Mandatory access control
B. Separation of duties access control
C. Discretionary access control
D. Role based access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 19
CompTIA SY0-301 Exam

QUESTION 73
A username provides which of the following?

A. Biometrics
B. Identification
C. Authorization
D. Authentication

Correct Answer: B
Section: (none)
Explanation

QUESTION 74
Use of group accounts should be minimized to ensure which of the following?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 75
Privilege creep among long-term employees can be mitigated by which of the following procedures?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 76
In which of the following scenarios is PKI LEAST hardened?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 77
A database server has been compromised via an unpatched vulnerability. An investigation reveals that an application crashed at the time of the compromise. Unauthorized code appeared to be running, although there were no traces of the code found on the file system. Which of the following attack types has MOST

likely occurred?

A. Zero day exploit

B. SQL injection
C. LDAP injection
D. Buffer overflow

Correct Answer: D
Section: (none)
Explanation

QUESTION 78
Which of the following would Sara, a security administrator, utilize to actively test security controls within an organization?

A. Penetration test
B. Baselining
C. Code review
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

QUESTION 79
Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 80
Which of the following would Jane, a security administrator, take advantage of to bypass security controls and gain unauthorized remote access into an organization?

A. Vulnerability scan
B. Dumpster diving
C. Virtualization
D. Penetration test

Correct Answer: D
Section: (none)
Explanation

QUESTION 81
Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

A. Penetration test
B. Code review
C. Vulnerability scan
D. Brute Force scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 21
CompTIA SY0-301 Exam

QUESTION 82
The finance department is growing and needs additional computers to support growth. The department also needs to ensure that their traffic is separated from the rest of the network. Matt, the security administrator, needs to add a new switch to accommodate this growth. Which of the following MUST Matt configure on the switch to ensure proper network separation?

A. Implicit deny
B. VLAN management
C. Access control lists
D. Flood guards

Correct Answer: B
Section: (none)
Explanation

QUESTION 83
Pete, the security administrator, wants to ensure that only secure protocols are being used to transfer and copy files. Which of the following protocols should he implement?

A. SMTP
B. SCP
C. FTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

QUESTION 84
Sara, a security administrator, has recently implemented a policy to ban certain attachments from being sent through the corporate email server. This is an example of trying to mitigate which of the following?

A. SQL injection

B. LDAP injection
C. Cross-site scripting
D. Malicious add-ons

Correct Answer: D
Section: (none)
Explanation

QUESTION 85
Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports
B. Use channels 1, 4 and 7 only
C. Enable MAC filtering
D. Disable SSID broadcast
E. Switch from 802.11a to 802.11b

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 22
CompTIA SY0-301 Exam

QUESTION 86
In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

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

Correct Answer: AD
Section: (none)
Explanation

QUESTION 87
Which of the following is used to certify intermediate authorities in a large PKI deployment?

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

Correct Answer: A
Section: (none)

Explanation

QUESTION 88
Which of the following components MUST be trusted by all parties in PKI?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 89
Remote employees login to the network using a device displaying a digital number which changes every five minutes. This is an example of which of the following?

A. Block cipher
B. One-time pad
C. Stream cipher
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

QUESTION 90
When checking his webmail, Matt, a user, changes the URL's string of characters and is able to get into another user's inbox. This is an example of which of the following?

A. Header manipulation
B. SQL injection
C. XML injection
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

QUESTION 91
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 92
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 93
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 94
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 95
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 96
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 97
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 98
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

QUESTION 99
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 100
Which of the following can use RC4 for encryption? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

QUESTION 101
Which of the following defines a business goal for system restoration and acceptable data loss?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 102
Which of the following defines an organization goal for acceptable downtime during a disaster or other contingency?

A. MTBF
B. MTTR
C. RTO
D. RPO

Correct Answer: C
Section: (none)
Explanation

QUESTION 103
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access
B. Dial-up access
C. Changing environmental controls
"First Test, First Pass" - www.lead2pass.com 26
CompTIA SY0-301 Exam
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

QUESTION 104
An ACL placed on which of the following ports would block IMAP traffic?

A. 110
B. 143
C. 389
D. 465

Correct Answer: B
Section: (none)
Explanation

QUESTION 105
Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast
B. MAC filtering
C. WPA2
D. Packet switching

Correct Answer: C
Section: (none)
Explanation

QUESTION 106
A new AP has been installed and there are problems with packets being dropped. Which of the following BEST explains the packet loss?

A. EMI
B. XML injection
C. DDoS
D. Botnet

Correct Answer: A

Section: (none)
Explanation

QUESTION 107
Which of the following intrusion 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
D. Behavioral

Correct Answer: D
Section: (none)
Explanation

QUESTION 108
Which of the following controls should be used to verify a person in charge of payment processing

is not colluding with anyone to pay fraudulent invoices?

A. Least privilege
B. Security policy
C. Mandatory vacations
D. Separation of duties

Correct Answer: C
Section: (none)
Explanation

QUESTION 109
Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

A. Least privilege
B. Sandboxing
C. Black box
D. Application hardening

Correct Answer: B
Section: (none)
Explanation

QUESTION 110
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent

B. Certificate authority
C. Trust model
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

QUESTION 111
Which of the following security methods should be used to ensure mobile devices are not removed by unauthorized users when the owner is away from their desk?

A. Screen lock
B. Biometrics
C. Strong passwords
D. Cable lock

Correct Answer: D
Section: (none)
Explanation

QUESTION 112
Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

A. Single sign on
B. IPv6
C. Secure zone transfers
"First Test, First Pass" - www.lead2pass.com 28
CompTIA SY0-301 Exam
D. VoIP

Correct Answer: C
Section: (none)
Explanation

QUESTION 113
Jane, a network technician, notices that users' Internet homepages have been changed to sites that include malware. Which of the following will change the default homepage for the Internet browser to be the same for all users?

A. Flush the DNS cache
B. Remove workstations from the domain
C. Upgrade the Internet browser
D. Implement group policies

Correct Answer: D
Section: (none)
Explanation

QUESTION 114
A security administrator wants to scan an infected workstation to understand how the infection occurred. Which of the following should the security administrator do FIRST before scanning the workstation?

A. Make a complete hard drive image
B. Remove the memory
C. Defragment the hard drive
D. Delete all temporary Internet files

Correct Answer: A
Section: (none)
Explanation

QUESTION 115
Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 116
The lead security engineer has been brought in on a new software development project. The software development team will be deploying a base software version and will make multiple software revisions during the project life cycle. The security engineer on the project is concerned with the ability to roll back software changes that cause bugs and/or security concerns. Which of the following should the security engineer suggest to BEST address this issue?

A. Develop a change management policy incorporating network change control.
B. Develop a change management policy incorporating hardware change control.
C. Develop a change management policy incorporating software change control.

D. Develop a change management policy incorporating oversight of the project lifecycle.

Correct Answer: C
Section: (none)
Explanation

QUESTION 117
A new wireless network was installed in an office building where there are other wireless networks. Which of the following can the administrator disable to help limit the discovery of the new network?

A. DHCP
B. Default user account
C. MAC filtering

D. SSID broadcast

Correct Answer: D
Section: (none)
Explanation

QUESTION 118
Which of the following anti-malware solutions can be implemented to mitigate the risk of phishing?

A. Host based firewalls
B. Anti-spyware
C. Anti-spam
D. Anti-virus

Correct Answer: C
Section: (none)
Explanation

QUESTION 119
Which of the following can be used to mitigate risk if a mobile device is lost?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 120
Implementation of server clustering is an example of which of the following security concepts?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 121
The annual loss expectancy can be calculated by:

A. dividing the annualized rate of return by single loss expectancy.
B. multiplying the annualized rate of return and the single loss expectancy.

C. subtracting the single loss expectancy from the annualized rate of return.
D. adding the single loss expectancy and the annualized rate of return.

Correct Answer: B
Section: (none)
Explanation

QUESTION 122
Which of the following datacenter environmental controls must be properly configured to prevent equipment failure from water?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 123
Which of the following should the security administrator do when taking a forensic image of a hard drive?

A. Image the original hard drive, hash the image, and analyze the original hard drive.
B. Copy all the files from the original into a separate hard drive, and hash all the files.
C. Hash the original hard drive, image the original hard drive, and hash the image.
D. Image the original hard drive, hash the original hard drive, and analyze the hash.

Correct Answer: C
Section: (none)
Explanation

QUESTION 124
In order to prevent and detect fraud, which of the following should be implemented?

A. Job rotation
B. Risk analysis
C. Incident management
D. Employee evaluations

Correct Answer: A
Section: (none)
Explanation

QUESTION 125
A vulnerability scan detects an unpatched application that does not exist on the server. Which of the following is the BEST explanation?

A. File corruption
B. False positive

C. Wrong system was scanned
D. Signature needs to be updated on the tool

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 31
CompTIA SY0-301 Exam

QUESTION 126
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 127
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

QUESTION 128
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 129

Mike, a system administrator, anticipating corporate downsizing this coming November writes a malicious program to execute three weeks later if his account is removed. Which of the following attacks is this?

A. Rootkit
B. Virus
C. Logic Bomb
D. Worm

Correct Answer: C
Section: (none)
Explanation

QUESTION 130
The Compliance Department implements a policy stating the Security Analyst must only review

security changes and the Security Administrator will implement the changes. This is example of which of the following?

A. Job rotation
B. Discretionary access control
C. Trust models
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

QUESTION 131
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 132
Which of the following protocols would be used to verify connectivity between two remote devices at the LOWEST level of the OSI model?

A. DNS
B. SCP
C. SSH
D. ICMP

Correct Answer: D
Section: (none)
Explanation

QUESTION 133
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 134
Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card
B. Role based access control

C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

QUESTION 135
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 136
Matt, the security administrator, notices a large number of alerts on the NIDS. Upon further inspection, it is determined that no attack has really taken place. This is an example of a:

A. false negative.
B. true negative.
C. false positive.
D. true positive.

Correct Answer: C
Section: (none)
Explanation

QUESTION 137
Sara, a visitor, plugs her Ethernet cable into an open jack in a wall outlet and is unable to connect to the network. This is MOST likely an example of:

A. port security.
B. implicit deny.
C. flood guards.
D. loop protection.

Correct Answer: A
Section: (none)
Explanation

QUESTION 138
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 34
CompTIA SY0-301 Exam

QUESTION 139
The security principle that is targeted when implementing ACLs is:

A. integrity.
B. availability.
C. confidentiality.
D. responsibility.

Correct Answer: C
Section: (none)
Explanation

QUESTION 140
Which of the following is true about two security administrators who are using asymmetric encryption to send encrypted messages to each other?

A. When one encrypts the message with the private key, the other can decrypt it with the private key.
B. When one encrypts the message with the private key, the other can decrypt it with the public key.
C. When one encrypts the message with the public key, the other can use either the public or the private to decrypt it.
D. When one encrypts the message with the public key, the other can decrypt it with the public key.

Correct Answer: B
Section: (none)
Explanation

QUESTION 141
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 142
Which of the following top to bottom sequential firewall rules will allow SSH communication?

A. DENY ANY ANY
PERMIT ANY ANY TCP 22
PERMIT ANY ANY UDP 22
B. PERMIT ANY ANY UDP 22
PERMIT ANY ANY TCP 21
DENY ANY ANY
C. PERMIT ANY ANY TCP 23
PERMIT ANY ANY TCP 22
DENY ANY ANY
"First Test, First Pass" - www.lead2pass.com 35
CompTIA SY0-301 Exam
D. PERMIT ANY ANY TCP 23
DENY ANY ANY
PERMIT ANY ANY TCP 22

Correct Answer: C
Section: (none)
Explanation

QUESTION 143
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 144
Which of the following Data Loss Prevention strategies is used to ensure that unauthorized users cannot access information stored in specified fields?

A. Whole disk encryption
B. Trust models
C. Database encryption
D. Individual file encryption

Correct Answer: C
Section: (none)
Explanation

QUESTION 145
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

QUESTION 146
Which of the following protocols would be implemented to secure file transfers using SSL?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Which of the following security concepts are used for data classification and labeling to protect data? (Select TWO).

A. Need to know
B. Role based access control
C. Authentication
D. Identification
E. Authorization

Correct Answer: AE
Section: (none)
Explanation

QUESTION 148
Which of the following cryptography concepts describes securing a file during download?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 149
Which of the following secure file transfer methods uses port 22 by default?

A. FTPS
B. SFTP
C. SSL
D. S/MIME

Correct Answer: B
Section: (none)
Explanation

QUESTION 150
A drawback of utilizing unmonitored proximity badge readers is that they perform:

A. authentication without authorization.
B. authorization with authentication.
C. authorization without authentication.
D. authentication with authorization.

Correct Answer: C
Section: (none)
Explanation

QUESTION 151
While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

A. EAP-TLS
B. PEAP
"First Test, First Pass" - www.lead2pass.com 37
CompTIA SY0-301 Exam
C. WEP
D. WPA

Correct Answer: C
Section: (none)
Explanation

QUESTION 152
Pete, a security administrator, instructs the networking team to push out security updates for a suite of programs on client workstations. This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 153
A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?

A. Succession planning
B. Fault tolerance
C. Continuity of operations
D. Removing single points of failure

Correct Answer: C
Section: (none)
Explanation

QUESTION 154
Sara, a security administrator, has implemented outbound email filtering. Which of the following would this MOST likely protect Sara's company from?

A. Data loss
B. Phishing
C. SPAM solicitation
D. Distributed denial of service attacks

Correct Answer: A
Section: (none)
Explanation

QUESTION 155
Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?

A. The web server is configured on the firewall's DMZ interface.
B. The VLAN is improperly configured.
C. The firewall's MAC address has not been entered into the filtering list.
D. The firewall executes an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 38
CompTIA SY0-301 Exam

QUESTION 156
Sara, the network security administrator, wants to separate Finance department traffic from the rest of the company. The company uses the following IP addresses:

Servers and switches: 192.168.1.1 - 192.168.1.40
Users: 192.168.1.70 - 192.168.1.110
Finance Users: 192.168.1.200 - 192.168.1.250

Which of the following would BEST meet Sara's goal?

A. Separate Gateways and Subnet mask of 255.255.255.254
B. VLAN and Subnet mask of 255.255.255.252
C. QoS and Subnet mask of 255.255.255.254
D. SwitchPort Security and a Subnet mask of 255.255.255.252

Correct Answer: B
Section: (none)
Explanation

QUESTION 157
Which of the following ports are used for secure SNMP and FTPS by default? (Select TWO).

A. 21
B. 22
C. 123
D. 161
E. 443
F. 8080

Correct Answer: DE

Section: (none)
Explanation

QUESTION 158
Which of the following wireless security algorithms is vulnerable to dictionary attacks when weak passwords are used?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 159
Power and data cables from the network center travel through the building's boiler room. Which of the following should be used to prevent data emanation?

A. Video monitoring
B. EMI shielding
C. Plenum CAT6 UTP
D. Fire suppression
"First Test, First Pass" - www.lead2pass.com 39
CompTIA SY0-301 Exam

Correct Answer: B
Section: (none)
Explanation

QUESTION 160
Mike, a user, receives an email from his grandmother stating that she is in another country and needs money. The email address belongs to his grandmother. Which of the following attacks is this?

A. Man-in-the-middle
B. Spoofing
C. Relaying
D. Pharming

Correct Answer: B
Section: (none)
Explanation

QUESTION 161
Sara, a user, receives several unwanted instant messages. Which of the following types of attacks is this?

A. Phishing
B. Vishing
C. Spam

D. Spim

Correct Answer: D
Section: (none)
Explanation

QUESTION 162
Sara, a security administrator, has changed access point signal strength and antenna placement to help prevent which of the following wireless attacks?

A. Evil twin
B. War driving
C. Bluesnarfing
D. IV attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 163
Which of the following ports is MOST likely using a secure protocol, by default?

A. 21
B. 80
C. 110
D. 443

Correct Answer: D
Section: (none)
Explanation

QUESTION 164
"First Test, First Pass" - www.lead2pass.com 40
CompTIA SY0-301 Exam

Which of the following network ports is MOST likely associated with HTTPS, by default?

A. 53
B. 80
C. 123
D. 443

Correct Answer: D
Section: (none)
Explanation

QUESTION 165
Which of the following allows Mike, a security technician, to view network traffic for analysis?

A. Spam filter

B. Sniffer
C. Router
D. Switch

Correct Answer: B
Section: (none)
Explanation

QUESTION 166
Which of the following should Matt, a security technician, apply to the network for loop protection?

A. Spanning tree
B. Log analysis
C. Implicit deny
D. Load balancers

Correct Answer: A
Section: (none)
Explanation

QUESTION 167
Which of the following network administration principles is MOST closely associated with firewall ACLs?

A. Log analysis
B. Port address translation
C. Implicit deny
D. Stateful inspection

Correct Answer: C
Section: (none)
Explanation

QUESTION 168
Which of the following protocols can be used to secure traffic for telecommuters?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 41
CompTIA SY0-301 Exam

QUESTION 169
Which of the following should Sara, a security technician, use to reduce the possibility of an attacker discovering the company's wireless network?

A. Disable SSID broadcast
B. Implement TKIP
C. Apply MAC filtering
D. Upgrade WEP to WPA

Correct Answer: A
Section: (none)
Explanation

QUESTION 170
Which of the following is a management control?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 171
Which of the following risk concepts BEST supports the identification of fraud?

A. Risk transference
B. Management controls
C. Mandatory vacations
D. Risk calculation

Correct Answer: C
Section: (none)
Explanation

QUESTION 172
Which of the following incident response aspects allows Pete, the security technician, to identify who caused a Distributed Denial of Service (DDoS) attack?

A. Network logs
B. Live system image
C. Record time offset
D. Screenshots

Correct Answer: A
Section: (none)
Explanation

QUESTION 173
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies
"First Test, First Pass" - www.lead2pass.com 42
CompTIA SY0-301 Exam
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

QUESTION 174
Which of the following must Mike, a user, implement if he wants to send a secret message to Jane, a co-worker, by embedding it within an image?

A. Transport encryption
B. Steganography
C. Hashing
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

QUESTION 175
In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 176
Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?

A. Intrusion prevention system
B. Web security gateway
C. Network access control
D. IP access control lists

Correct Answer: C
Section: (none)
Explanation

QUESTION 177
Mike, a server engineer, has received four new servers and must place them in a rack in the datacenter. Which of the following is considered best practice?

A. All servers' air exhaust toward the cold aisle.
B. All servers' air intake toward the cold aisle.
C. Alternate servers' air intake toward the cold and hot aisle.
D. Servers' air intake must be parallel to the cold/hot aisles.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 43
CompTIA SY0-301 Exam

QUESTION 178
Mike, a security analyst, has captured a packet with the following payload:

GET ../../../../system32\/cmd.exe

Which of the following is this an example of?

A. SQL injection
B. Directory traversal
C. XML injection
D. Buffer overflow

Correct Answer: B
Section: (none)
Explanation

QUESTION 179
Sara, the security administrator, needs to open ports on the firewall to allow for secure data transfer. Which of the following TCP ports would allow for secure transfer of files by default?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 180
Which of the following technologies would allow for a secure tunneled connection from one site to another? (Select TWO).

A. SFTP

B. IPSec
C. SSH
D. HTTPS
E. ICMP

Correct Answer: BC
Section: (none)
Explanation

QUESTION 181
Which of the following sets numerous flag fields in a TCP packet?

A. XMAS
B. DNS poisoning
C. SYN flood
D. ARP poisoning

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 182
Which of the following devices is MOST commonly used to create a VLAN?

A. Hub
B. Router
C. Firewall
D. Switch

Correct Answer: D
Section: (none)
Explanation

QUESTION 183
Which of the following network design elements provides for a one-to-one relationship between an internal network address and an external network address?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 184

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

A. impersonation.
B. tailgating.
C. dumpster diving.
D. shoulder surfing.

Correct Answer: D
Section: (none)
Explanation

QUESTION 185
In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic patterns?

A. Syslog
B. Protocol analyzer
C. Proxy server
D. Firewall

Correct Answer: B
Section: (none)
Explanation

QUESTION 186
Jane, a security administrator, has asked her technicians to determine if a certificate is valid. Which of the following should be checked to determine whether or not a certificate has been invalidated?

A. CA

B. CRL
C. PKI
D. CRC

Correct Answer: B
Section: (none)
Explanation

QUESTION 187
TKIP uses which of the following encryption ciphers?

A. RC5
B. AES
C. RC4
D. 3DES

Correct Answer: C
Section: (none)
Explanation

QUESTION 188
The process of exchanging public keys is BEST explained as which cryptography concept?

A. Symmetric encryption
B. Asymmetric encryption
C. Key escrow
D. Transport encryption

Correct Answer: B
Section: (none)
Explanation

QUESTION 189
Which of the following network segments would be BEST suited for installing a honeypot?

A. Management network
B. Internal network
C. External network
D. DMZ network

Correct Answer: C
Section: (none)
Explanation

QUESTION 190
Jane, a security architect, has noticed significant performance loss with the increase in user-base of her PKI infrastructure. Which of the following could she deploy in order to increase response times?

A. Smart card
B. CAC
C. HSM
D. VPN

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 191
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

QUESTION 192
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 193
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 194
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

Explanation/Reference:

QUESTION 195
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 196
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 197
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 198
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 199
"First Test, First Pass" - www.lead2pass.com 48
CompTIA SY0-301 Exam

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 200
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 201
Which of the following is a secure alternate to Telnet?

A. TFTP
B. HTTPS
C. SSH
D. SCP

Correct Answer: C
Section: (none)
Explanation

QUESTION 202
Temporary employees are not allowed to work overtime. The information security department must implement a control to enforce this measure. Which of the following measures would BEST enforce this policy?

A. Separation of duties
B. Personal identification card
C. Single sign-on
D. Time of day restrictions

Correct Answer: D
Section: (none)
Explanation

QUESTION 203
Sara from IT Governance wants to provide a mathematical probability of an earthquake using facts and figures. Which of the following concepts would achieve this?

A. Qualitative Analysis
B. Impact Analysis

C. Quantitative Analysis
D. SLE divided by the ARO

Correct Answer: C
Section: (none)
Explanation

QUESTION 204
During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

A. All users have write access to the directory.
B. Jane has read access to the file.
C. All users have read access to the file.
D. Jane has read access to the directory.

Correct Answer: C
Section: (none)
Explanation

QUESTION 205
Sara, an IT security technician, is actively involved in identifying coding issues for her company. Which of the following is an application security technique that she can use to identify unknown weaknesses within the code?

A. Vulnerability scanning
B. Denial of service
C. Fuzzing
D. Port scanning

Correct Answer: C
Section: (none)
Explanation

QUESTION 206
Sara, an IT security technician, has identified security weaknesses within her company's code. Which of the following is a common security coding issue?

A. Input validation
B. Application fuzzing
C. Black box testing
D. Vulnerability scanning

Correct Answer: A
Section: (none)
Explanation

QUESTION 207
Which of the following is an application security coding problem?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 50
CompTIA SY0-301 Exam

QUESTION 208
Pete, an IT security technician, needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 209
Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration?

A. Hard drive encryption
B. Infrastructure as a service
C. Software based encryption
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

QUESTION 210
Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 211
Which of the following is based on asymmetric keys?

A. CRLs
B. Recovery agent
C. PKI
D. Registration

Correct Answer: C
Section: (none)
Explanation

QUESTION 212
Which of the following is BEST described as a notification control, which is supported by other identification controls?

A. Fencing
B. Access list
C. Guards
D. Alarm

Correct Answer: D
Section: (none)
Explanation

QUESTION 213
Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

A. Certification authority

B. Key escrow
C. Certificate revocation list
D. Registration authority

Correct Answer: A
Section: (none)
Explanation

QUESTION 214
Which of the following BEST describes the weakness in WEP encryption?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 215
Which of the following is used to ensure message integrity during a TLS transmission?

A. RIPEMD
B. RSA
C. AES
D. HMAC

Correct Answer: D
Section: (none)
Explanation

QUESTION 216
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.

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

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 217
A company has asked Pete, a penetration tester, to test their corporate network. Pete was provided with all of the server names, configurations, and corporate IP addresses. Pete was then instructed to stay off of the Accounting subnet as well as the company web server in the DMZ. Pete was told that social engineering was not in the test scope as well. Which of the following BEST describes this penetration test?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 218
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 219
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 220
Pete, a security engineer, maintains up-to-date virus scan signatures on all systems. Which of the following should Pete do as well to prevent the exploiting of known vulnerabilities?

A. Application patching
B. White box penetration testing
C. Vulnerability assessment
D. Port scanning

Correct Answer: A
Section: (none)
Explanation

QUESTION 221
If Pete, the administrator, is blocking port 69, which of the following protocols will this affect?

A. TFTP
B. FTP
C. RDP
D. DNS

Correct Answer: A
Section: (none)
Explanation

QUESTION 222
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system
B. Electrical
C. HVAC
D. Video surveillance

Correct Answer: C
Section: (none)
Explanation

QUESTION 223
Pete, a home user, is trying to secure his wireless network from his technical neighbor. Which of the following should Pete implement on his access point to keep his neighbor from accessing his wireless network and viewing Pete's online chats?

A. WPA
B. RIPEMD
C. WEP
D. LEAP

Correct Answer: A
Section: (none)
Explanation

QUESTION 224

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

A. Hardware load balancing
B. RAID
C. A cold site
D. A host standby
"First Test, First Pass" - www.lead2pass.com 54
CompTIA SY0-301 Exam

Correct Answer: B
Section: (none)
Explanation

QUESTION 225
Pete has obtained a highly sensitive document and has placed it on a network drive which has been formatted with NTFS and is shared via CIFS. Which of the following access controls apply to the sensitive file on the server?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 226
Matt, the backup operator, is implementing a new backup plan. Which of the following is the MOST important step in a backup plan to ensure the disaster recovery plan is executed without any incidents?

A. Verify that the data on the backup tapes can be restored on a test server.
B. Verify that the backup plan is stored in digital format on the backup tapes.
C. Verify that the data on the backup tapes can be restored on the web server.
D. Verify that all backup data is encrypted on the tape and store the encryption key offsite.

Correct Answer: A
Section: (none)
Explanation

QUESTION 227
Which of the following information should Pete, an employee at a pharmaceutical company, review during the company-wide information security awareness training, before handling customer data?

A. Acceptable use policy
B. Account management procedures
C. Laws and regulations
D. End user license agreement

Correct Answer: A
Section: (none)
Explanation

QUESTION 228
Matt has installed a new KDC for his corporate environment. Which of the following authentication protocols is Matt planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 55
CompTIA SY0-301 Exam

QUESTION 229
Which of the following uses only a private key?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 230
Sara, a security manager, received the results of a vulnerability assessment stating that several accounts were enabled, even though the employees had been terminated in months prior. Which of the following needs to be performed to ensure this issue is mitigated for future tests?

A. Change management reviews
B. Routine account audits
C. Incident management audits
D. User rights and permissions reviews

Correct Answer: B
Section: (none)
Explanation

QUESTION 231
Matt, a security manager, receives the results of a social engineering exercise. An attacker was able to successfully impersonate Sara, a company executive, over the phone when contacting the helpdesk and gained access to her password. After further research, it was determined that someone in the company had thrown out printouts of Sara's calendar for that week, showing when she would be traveling on business.

Which of the following should employees be trained on to help mitigate this issue in the future?

A. Password behaviors
B. Help desk procedures
C. Secure disposal policy
D. Clean desk policies

Correct Answer: C
Section: (none)
Explanation

QUESTION 232
Sara is sniffing traffic on a wireless network configured with WEP. She obtains numerous packets and then attempts to breach the network. Which of the following is Sara MOST likely attempting?

A. Bluejacking
B. IV attack
C. Evil twin
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 56
CompTIA SY0-301 Exam

QUESTION 233
Matt, a security technician, has been tasked with updating client anti-virus solutions. He makes sure that all of the workstations have been properly updated. Later that day, he receives a call from a user stating that their PC is unresponsive and the screen blanks out every few minutes. Matt goes to the website of the anti-virus vendor and sees that new virus definitions are available. Which of the following is the MOST likely cause of the behavior that the user is reporting?

A. A zero-day attack
B. IV attack
C. XML injection
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

QUESTION 234
Pete, a network administrator, needs to implement a VPN. Which of the following could he use to accomplish this objective? (Select TWO).

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

E. SCP
F. SFTP

Correct Answer: CD
Section: (none)
Explanation

QUESTION 235
Matt has recently implemented a new network design at his organization and wishes to actively test security controls on the new network. Which of the following should Matt perform?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 236
Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

A. Clustering
B. RAID
C. Load balancing
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 57
CompTIA SY0-301 Exam

QUESTION 237
Pete, an employee, was recently indicted for fraud charges. Jane, a new security technician at the company, was tasked with collecting information from Pete's workstation. Jane seized the hard drive from the workstation without collecting any other information from the workstation. Which of the following principles did Jane violate?

A. Track man hours and expense
B. Order of volatility
C. Damage control
D. Preservation of evidence

Correct Answer: B
Section: (none)
Explanation

QUESTION 238
A database server containing personal information and a file server containing non-critical information must be secured. Which of the following would be a BEST practice to secure the servers? (Select TWO).

A. Place the file server behind a door requiring biometric authorization.
B. Place both servers under the system administrator's desk.
C. Place the database server behind a door with a cipher lock.
D. Place the file server in an unlocked rack cabinet.
E. Place the database server behind a door requiring biometric authorization.

Correct Answer: AE
Section: (none)
Explanation

QUESTION 239
A company is experiencing an extraordinary amount of web traffic that is crippling the server. The web traffic suddenly stops. The mail server experiences the same amount of traffic as before then crashes. Which of the following attacks would this BEST describe?

A. DoS
B. Spam
C. Man-in-the-middle
D. Replay

Correct Answer: A
Section: (none)
Explanation

QUESTION 240
Which of the following would ensure confidentiality and authorization to the management interface of a router?

A. Enable an access list and RADIUS
B. Enable SSH and TACACS
C. Enable an access list and PKI
D. Enable LDAP and strong passwords

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 58
CompTIA SY0-301 Exam

QUESTION 241
Which of the following BEST describes a demilitarized zone?

A. A buffer zone between protected and unprotected networks.
B. A network where all servers exist and are monitored.
C. A sterile, isolated network segment with access lists.

D. A private network that is protected by a firewall and a VLAN.

Correct Answer: A
Section: (none)
Explanation

QUESTION 242
Which of the following statements BEST describes the basic functionality of a network firewall?

A. Improves communication between trusted and non-trusted networks
B. Redirects accepted traffic to the proper VLAN
C. Provides stateful packet inspection of TCP traffic
D. Accepts and rejects data based on content

Correct Answer: C
Section: (none)
Explanation

QUESTION 243
Which of the following BEST describes the function of a protocol analyzer?

A. It allows a security technician to decrypt packets as they traverse the network.
B. It allows a security technician to encrypt packets as they traverse the network.
C. It allows a security technician to perform deep state packet inspection.
D. It allows a security technician to perform hardware device troubleshooting.

Correct Answer: C
Section: (none)
Explanation

QUESTION 244
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 245
Which of the following network design elements BEST provides a testing environment to perform malware analysis?

A. Platform as a Service (PaaS)
B. DMZ
C. Virtualization

D. Proxies

Correct Answer: C
Section: (none)
Explanation

QUESTION 246
Matt, a security technician, is attempting to explain why some of the company policies should be changed for high risk IT positions. Which of the following concepts BEST explains his support for fraud detection?

A. Time of day restrictions is more likely to discover fraud than the other fraud detection methods.
B. Least privilege principles allow internal audit teams to discover fraud while a staff member is out of the office.
C. Separation of duties is a better fraud detection method than mandatory vacations; therefore, it should be used.
D. Mandatory vacations support the company discovering fraud while staff members are out of the office.

Correct Answer: D
Section: (none)
Explanation

QUESTION 247
Jane, a security technician, is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks Jane to explain the access control type found in a firewall. With which of the following should Jane respond?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 248
Sara, a security administrator, has been tasked with explaining smart cards to the company's management team. Which of the following are smart cards? (Select TWO).

A. DAC
B. Tokens
C. CAC
D. ACL
E. PIV

Correct Answer: CE
Section: (none)
Explanation

QUESTION 249
Jane, a security architect, is implementing security controls throughout her organization. Which of the following BEST explains the vulnerability in the formula that a Risk = Threat x Vulnerability x Impact?

A. Vulnerability is related to the risk that an event will take place.
B. Vulnerability is related to value of potential loss.
C. Vulnerability is related to the probability that a control will fail.
D. Vulnerability is related to the probability of the event.

Correct Answer: C
Section: (none)
Explanation

QUESTION 250
Jane, a security analyst, has recently implemented a password complexity requirement within the company systems. Which of the following BEST explains this requirement?

A. Accounts shall be required to adhere to no less than 15 characters for all personnel accounts.
B. Accounts shall have two uppercase, two lowercase, and one number or special character.
C. Accounts shall be changed no less than every ninety (90) days for service accounts.
D. Accounts shall be disabled after a period of thirty (30) days if the account has not logged on within that time period.

Correct Answer: B
Section: (none)
Explanation

QUESTION 251
Pete, an email administrator, notices that Sara and Matt are exchanging image files back and forth. Pete opens an image and sees the image is from the company's intranet. Pete checks the MD5 hash of the file on the Internet page versus the file Sara and Matt are sending and the hash values do not match. Which of the following is this MOST likely an example of?

A. Key escrow
B. Steganography
C. Digital signature
D. Non-repudiation

Correct Answer: B
Section: (none)
Explanation

QUESTION 252
The HR department has been rotating positions in their own department and hiring new employees to fill positions. It is the end of the year and Pete, the CEO, is concerned about performance reviews and salaries being leaked from the corporate file server. Which of the following should Pete request be done to ensure only the required employees have access to the performance reviews?

A. Perform an audit for access.
B. Encrypt the data.
C. Check the logs for access.
D. Move the data to a USB drive.

Correct Answer: A
Section: (none)
Explanation

QUESTION 253
Jane is building a new web server. Jane only wants to run a web server on a workstation so she disables the default web site, turns off FTP, adds a certificate, and enables port 443 on the web

server. Jane is performing which of the following?

A. Application patch management
B. Exception handling
C. Application hardening
D. Application baselining

Correct Answer: C
Section: (none)
Explanation

QUESTION 254
Pete's boss is concerned with the amount of down time the shipping and receiving server is having. He asks Pete to provide him with numbers on the mean time between failures. Which of the following equations could Pete perform to provide this information to his boss?

A. Calculate the Annual Loss Expectancy for the year.
B. Track the man hours and expenses of the system being down for a month.
C. The operational time of the server divided by the number of times the system went down.
D. Calculate the Annual Rate of Occurrence for the year.

Correct Answer: C
Section: (none)
Explanation

QUESTION 255
The information security department regularly walks the campus and around the buildings looking for unauthorized open wireless networks. This is an example of which of the following?

A. A site survey
B. Antenna placement
C. War dialing
D. War driving

Correct Answer: D
Section: (none)
Explanation

QUESTION 256
Sara, an attacker, launches a man-in-the-middle attack against Pete. While sniffing Pete's network traffic, Sara is able to acquire the current cookies Pete is using. Which of the following can Sara use these cookies for?

A. Buffer overflow
B. Header manipulation
C. ARP poisoning
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

QUESTION 257
Users are reporting having trouble connecting to a certain web server. Pete, the security engineer, discovers the server appears to be running optimally at the OS level. Upon deeper investigation, Pete determines that the server is suspiciously flooding users with RST packets when they attempt to connect. Which of the following tools did Pete MOST likely use to discover this?

A. Honeynet
B. Network sniffer
C. Vulnerability scanner
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

QUESTION 258
The lobby of the hotel allows users to plug in their laptops to access the Internet. This network is also used for the IP based phones in the hotel lobby. Mike, the security engineer, wants to secure the phones so that guests cannot electronically eavesdrop on other guests. Which of the following would Mike MOST likely implement?

A. VLAN
B. Port security
C. MPLS
D. Separate voice gateway

Correct Answer: A
Section: (none)
Explanation

QUESTION 259
Jane, the security engineer, is tasked with hardening routers. She would like to ensure that network access to the corporate router is allowed only to the IT group and from authorized machines. Which of the following would MOST likely be implemented to meet this security goal? (Select TWO).

A. SNMP
B. HTTPS
C. ACL
D. Disable console
E. SSH
F. TACACS+

Correct Answer: CF
Section: (none)
Explanation

QUESTION 260
Jane, the network administrator, would like wireless users to authenticate to the network's RADIUS server via EAP prior to connecting to the WLAN. Which of the following would MOST likely be implemented to facilitate this authentication?

A. 802.1x
B. WPA2-PSK
C. WEP
D. TACACS+

Correct Answer: A
Section: (none)
Explanation

QUESTION 261
"First Test, First Pass" - www.lead2pass.com 63
CompTIA SY0-301 Exam

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 262
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 263
Pete, the system administrator, has concerns regarding users losing their company provided smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns?

A. Enforce device passwords.
B. Use remote sanitation.
C. Enable GPS tracking.
D. Encrypt stored data.

Correct Answer: C
Section: (none)
Explanation

QUESTION 264
Pete, the system administrator, wishes to monitor and limit users' access to external websites. Which of the following would BEST address this?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 265
Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 266
An external company has notified Jane at ABC Co. that their web server was attacked by one of ABC's IP addresses. The external company provides the time of the attack and the following log information:

SRC IP: 182.45.88.12
SRC Port: TCP 1335
DST IP: 12.42.8.122
DST Port: TCP 443

Given that ABC uses PAT at their firewall, which of the following is true about this incident?

A. Jane cannot identify the ABC's internal IP address that launched the attack because it happened over HTTPS.
B. The external company must provide the packet payload in order for Jane to identify the ABC's IP that launched the attack.
C. The external company did not provide enough information for Jane to be able to identify the ABC's internal IP that launched the attack.
D. Jane can identify the ABC's internal IP address that launched the attack by reviewing the Firewall logs.

Correct Answer: D
Section: (none)
Explanation

QUESTION 267
Which of the following settings can Jane, the network administrator, implement in the computer lab to ensure that user credentials cannot be captured by the next computer user?

A. Implement full drive encryption on all lab computers.
B. Reverse the computer to its original state upon reboot.
C. Do not display last username in logon screen.
D. Deploy privacy screens on all lab computers.

Correct Answer: C
Section: (none)
Explanation

QUESTION 268
Jane, a security administrator, is reviewing the company's official documentation to mitigate the risk of data loss due to personally owned devices being connected to perform company related work. Which of the following documentation should Jane MOST likely review and update?

A. Acceptable risk
B. Data retention policy
C. Acceptable use policy
D. End user license agreement

Correct Answer: C
Section: (none)
Explanation

QUESTION 269
After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

A. Succession planning
B. Disaster recovery plan
C. Information security plan
D. Business impact analysis

Correct Answer: B
Section: (none)
Explanation

QUESTION 270
Pete, a security administrator, has implemented SSH across all network infrastructure devices in the enterprise. Which of the following protocols will be used to exchange keying material within SSH?

A. Transport layer protocol
B. IPSec
C. Diffie-Hellman
D. Secure socket layer

Correct Answer: C
Section: (none)
Explanation

QUESTION 271
A user has just returned from security awareness training, where users were encouraged to strengthen their passwords and voicemail codes. Which of the following would be the MOST secure password for the user's workstation?

A. H0me0nTh3Range
B. Letme1nNow
C. $3cur1#y
D. Passw0rd99

Correct Answer: C
Section: (none)
Explanation

QUESTION 272
Matt must come up with a design solution which will enable remote users to securely access network resources. Which of the following design elements will enable Matt to meet this objective?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 66
CompTIA SY0-301 Exam

QUESTION 273
Sara, a security technician, has been asked to design a solution which will enable external users to have access to a Web server, while keeping the internal network unaffected by this access. Which of the following would BEST meet this objective?

A. Place the Web server on a VLAN
B. Place the Web server inside of the internal firewall
C. Place the Web server in a DMZ
D. Place the Web server on a VPN

Correct Answer: C
Section: (none)
Explanation

QUESTION 274
Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 275
A company that provides streaming media has recently experienced latency during certain times of the day. Which of the following would mitigate the latency issue?

A. Web security gateway
B. Firewall
C. Load balancing
D. VPN concentrator

Correct Answer: C
Section: (none)
Explanation

QUESTION 276
Matt, a security technician, notices a high number of ARP spoofing attacks on his network. Which of the following design elements would mitigate ARP spoofing attacks?

A. Flood guards

B. Implicit deny
C. VLANs
D. Loop protection

Correct Answer: A
Section: (none)
Explanation

QUESTION 277
Matt works for an organization that requires data to be recovered in the shortest amount of time possible. Which of the following backup types would BEST meet the organization's needs?

A. Full backups daily
B. Differential backups monthly
C. Full backups weekly
D. Incremental backups monthly

Correct Answer: A
Section: (none)
Explanation

QUESTION 278
How would a technician secure a router configuration if placed in an unsecured closet?

A. Mount the router into an immovable rack.
B. Enable SSH for maintenance of the router.
C. Disable the console port on the router.
D. Label the router with contact information.

Correct Answer: C
Section: (none)
Explanation

QUESTION 279
Which of the following firewall rules would only block tftp traffic and record it?

A. deny udp any server log
B. deny udp any server eq 69
C. deny tcp any server log
D. deny udp any server eq 69 log

Correct Answer: D
Section: (none)
Explanation

QUESTION 280
Which of the following services should be disabled to stop attackers from using a web server as a mail relay?

A. IMAP
B. SMTP
C. SNMP
D. POP3

Correct Answer: B
Section: (none)
Explanation

QUESTION 281
Mapping one IP address to another IP address is an example of:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 68
CompTIA SY0-301 Exam

QUESTION 282
A security administrator has a requirement to encrypt several directories that are non-hierarchical. Which of the following encryption models would BEST meet this requirement?

A. AES512
B. Database encryption
C. File encryption
D. Full disk encryption

Correct Answer: D
Section: (none)
Explanation

QUESTION 283
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are backdoors and logic bombs. Which of the following differentiates these two types of malware?

A. A backdoor is a coding issue that can be discovered by proper configuration management processes.
B. A logic bomb is typically hidden within the boot sector of the hard drive and is used to cause DDoS.
C. A backdoor is a third generation attack which is typically low risk because only highly trained staff can achieve it.
D. A logic bomb is undetectable by current antivirus signatures because a patch has not been issued.

Correct Answer: A
Section: (none)

Explanation

QUESTION 284
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

A. Viruses are a subset of botnets which are used as part of SYN attacks.
B. Botnets are a subset of malware which are used as part of DDoS attacks.
C. Viruses are a class of malware which create hidden openings within an OS.
D. Botnets are used within DR to ensure network uptime and viruses are not.

Correct Answer: B
Section: (none)
Explanation

QUESTION 285
Which of the following BEST explains the use of an HSM within the company servers?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 69
CompTIA SY0-301 Exam

QUESTION 286
Which of the following technologies can store multi-tenant data with different security requirements?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 287
Which of the following technologies prevents USB drives from being recognized by company systems?

A. Registry keys
B. Full disk encryption
C. USB encryption
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

QUESTION 288
Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 289
Which of the following types of encryption will help in protecting files on a PED?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 290
Which of the following is MOST closely associated with BitLocker?

A. ACL
B. DOS

C. DLP
D. TPM

Correct Answer: D
Section: (none)
Explanation

QUESTION 291
Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 292
Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 293
Which of the following presents the STRONGEST access control?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 294
Which of the following encompasses application patch management?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 295
Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 296
Which of the following is the LEAST volatile when performing incident response procedures?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 297
Which of the following can allow Sara, a security analyst, to encrypt individual files on a system?

A. EFS
B. Single sign-on
C. TLS
D. Journaled file system

Correct Answer: A
Section: (none)
Explanation

QUESTION 298
An encryption method where the plain text and cipher text are always the same size is an example of which of the following types of encryption?

A. RC4
B. MD5
C. Steam Cipher
D. Block Cipher

Correct Answer: D
Section: (none)
Explanation

QUESTION 299
The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST

protect people from which of the following?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 300
The compliance team comes out with a new policy that all data stored on tapes over 3 years must be degaussed. This BEST describes which of the following types of policies?

A. Data handling
B. Data classification
C. Data labeling
D. Data disposal

Correct Answer: D
Section: (none)
Explanation

QUESTION 301
Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number. Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 302
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

A. Interference

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 303
Jane, the security administrator, is having issues with unauthorized users connecting to the wireless network. For administrative reasons, she cannot implement any wireless encryption methods. Which of the following can she implement to prevent unauthorized users from

connecting to the network?

A. NIPS
B. Disable unused ports
C. MAC filtering
D. WEP

Correct Answer: C
Section: (none)
Explanation

QUESTION 304
Matt, the security administrator, wants to secure the wireless network. Which of the following encryption methods offers the MOST security?

A. WPA2 ENT AES
B. WPA2 PSK AES
C. WPA2 ENT TKIP
D. WPA2 PSK TKIP

Correct Answer: A
Section: (none)
Explanation

QUESTION 305
Sara, the IT administrator, wants to control which devices can connect to the wireless network. Which of the following can she implement to accomplish this task?

A. WPA2 Enterprise with AES encryption
B. Decrease the WAP's power levels
C. Static IP addressing
D. MAC address filtering

Correct Answer: D
Section: (none)

Explanation

QUESTION 306
When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

A. Humidity sensors
B. EMI shielding
C. Channel interference
D. Cable kinking

Correct Answer: B
Section: (none)
Explanation

QUESTION 307
Pete, the Chief Security Officer, wishes to institute annual security policy training for all users. The training's purpose is to educate users about access to sensitive data. Which of the following should be included in the training?

A. Revalidation of user account privileges.

B. Review of guidelines for network stored data permissions.
C. Implementation of new password procedures.
D. Installation of disk-based encryption to protect data.

Correct Answer: C
Section: (none)
Explanation

QUESTION 308
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 309
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 310
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 311
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 312
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 313
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 314
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 315
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 76
CompTIA SY0-301 Exam

QUESTION 316
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 an access log and a security guard
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: D
Section: (none)
Explanation

QUESTION 317
An administrator with a small company has begun to implement a backup strategy of the company's critical financial data. Which of the following is the MOST secure place to store the back-ups?

A. Near the data servers, for ease of restoration
B. Next to where the physical records (e.g. paper) are stored
C. At a remote off-site location
D. With the financial department

Correct Answer: C
Section: (none)
Explanation

QUESTION 318
In an enterprise environment, which of the following would be the BEST way to prevent users from accessing inappropriate websites when AUP requirements are constantly changing?

A. Deploy a network proxy server.
B. Configure Internet content filters on each workstation.
C. Deploy a NIDS.
D. Deploy a HIPS.

Correct Answer: A
Section: (none)
Explanation

QUESTION 319
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 320
A new wireless router has been compromised, blocking all of the company computers from using

the router. Which of the following is the MOST likely cause for this issue?

A. There was a backdoor account on the router.
B. The default password on the router was not changed.
C. The attacker discovered the WEP key of the router.
D. The attacker had gone dumpster diving to find the router's credentials.

Correct Answer: B
Section: (none)
Explanation

QUESTION 321
A company wants to maintain a backup site, and is more concerned about site maintenance cost rather than high availability following a disaster. Which of the following is the BEST solution?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 322
Which of the following would be the MOST likely reason to use a cluster of host servers to support load balancing?

A. Confidentiality by distributing traffic across multiple host servers
B. Enhance security by obscuring the physical host of the guest server
C. Availability by distributing connections across multiple servers
D. Integrity by separating traffic across multiple guest servers

Correct Answer: C
Section: (none)
Explanation

QUESTION 323
Which of the following controls is considered to be the MOST effective type of physical security?

A. Access lists
B. Cipher lock
C. Chain link fence
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

QUESTION 324
An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

A. Implement a password expiration policy.
B. Implement an account expiration date for permanent employees.
C. Implement time of day restrictions for all temporary employees.
D. Run a last logon script to look for inactive accounts.

Correct Answer: D
Section: (none)
Explanation

QUESTION 325
Which of the following devices is used to capture and analyze data packets when Jane, an unauthorized user, is trying to gain access to a network?

A. Sniffer
B. VPN concentrator
C. Packet filtering firewall
D. Router

Correct Answer: A
Section: (none)
Explanation

QUESTION 326
Which of the following is the BEST filtering device capable of stateful packet inspection?

A. Switch
B. Protocol analyzer
C. Firewall
D. Router

Correct Answer: C
Section: (none)
Explanation

QUESTION 327
An employee's workstation is connected to the corporate LAN. Due to content filtering restrictions, the employee attaches a 3G Internet dongle to get to websites that are blocked by the corporate gateway. Which of the following BEST describes a security implication of this practice?

A. A corporate LAN connection and a 3G Internet connection are acceptable if a host firewall is installed.
B. The security policy should be updated to state that corporate computer equipment should be dual-homed.
C. Content filtering should be disabled because it may prevent access to legitimate sites.
D. Network bridging must be avoided, otherwise it may join two networks of different classifications.

Correct Answer: D
Section: (none)
Explanation

QUESTION 328
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

A. Subnetting
B. NAT
C. Firewall
D. NAC
E. VPN

Correct Answer: CE
Section: (none)
Explanation

QUESTION 329
If a security issue is resolved, which of the following risk management strategies was used?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 330
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 331
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie

C. Pet's name
D. Birthday
E. Full name

Correct Answer: DE
Section: (none)
Explanation

QUESTION 332
In a disaster recovery situation, operations are to be moved to an alternate site. Computers and network connectivity are already present; however, production backups are several days out-of- date. Which of the following site types is being described?

A. Cold site
B. High availability site
C. Warm site
D. Hot site

Correct Answer: C
Section: (none)
Explanation

QUESTION 333
"First Test, First Pass" - www.lead2pass.com 80
CompTIA SY0-301 Exam

Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

A. Trojan
B. Pharming
C. Worms
D. Virus
E. Logic bomb

Correct Answer: BE
Section: (none)
Explanation

QUESTION 334
Which of the following threats corresponds with an attacker targeting specific employees of a company?

A. Spear phishing
B. Phishing
C. Pharming
D. Man-in-the-middle

Correct Answer: A
Section: (none)
Explanation

QUESTION 335
Which of the following attacks would password masking help mitigate?

A. Shoulder surfing
B. Brute force
C. Tailgating
D. Impersonation

Correct Answer: A
Section: (none)
Explanation

QUESTION 336
If cookies with non-random sequence numbers are issued upon authentication, which of the following attack types can occur?

A. Directory traversal
B. Session hijacking
C. Cross-site scripting
D. SQL injection

Correct Answer: B
Section: (none)
Explanation

QUESTION 337
Two systems are being designed. System A has a high availability requirement. System B has a high security requirement with less emphasis on system uptime. Which of the following configurations BEST fits the need for each system?

A. System A fails open. System B fails closed.

B. System A and System B both fail closed.
C. System A and System B both fail open.
D. System A fails closed. System B fails open.

Correct Answer: A
Section: (none)
Explanation

QUESTION 338
An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

A. Baseline reporting
B. Protocol analysis
C. Threat modeling
D. Functional testing

Correct Answer: A

Section: (none)
Explanation

QUESTION 339
Which of the following is a strong cryptographic system used by Windows based systems for authentication?

A. SSO
B. DES
C. NTLMv2
D. LANMAN

Correct Answer: C
Section: (none)
Explanation

QUESTION 340
Which of the following algorithms has well documented collisions? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

QUESTION 341
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

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 82
CompTIA SY0-301 Exam

QUESTION 342
Which of the following describes an issue encountered when reconstructing a security incident through the examination of security logs collected from multiple servers?

A. Proprietary log formats prevent review of security alerts
B. Some operating systems do not natively export security logs
C. Security logs are often encrypted

D. Inconsistent time settings interfere with sequential event analysis

Correct Answer: D
Section: (none)
Explanation

QUESTION 343
When verifying file integrity on a remote system that is bandwidth limited, which of the following tool combinations provides the STRONGEST confidence?

A. MD5 and 3DES
B. MD5 and SHA-1
C. SHA-256 and RSA
D. SHA-256 and AES

Correct Answer: B
Section: (none)
Explanation

QUESTION 344
Jane, the security administrator, needs to be able to test malicious code in an environment where it will not harm the rest of the network. Which of the following would allow Jane to perform this kind of testing?

A. Local isolated environment
B. Networked development environment
C. Infrastructure as a Service
D. Software as a Service

Correct Answer: A
Section: (none)
Explanation

QUESTION 345
A company is sending out a message to all users informing them that all internal messages need to be digitally signed. This is a form of which of the following concepts?

A. Availability
B. Non-repudiation
C. Authorization
D. Cryptography

Correct Answer: B
Section: (none)
Explanation

QUESTION 346
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

QUESTION 347
Which of the following are used to implement VPNs? (Select TWO).

A. SFTP
B. IPSec
C. HTTPS
D. SNMP
E. SSL

Correct Answer: BE
Section: (none)
Explanation

QUESTION 348
A company is concerned about physical laptop theft. Which of the following is the LEAST expensive way to prevent this threat?

A. Bollards
B. Full disk encryption
C. Cable locks
D. Safes

Correct Answer: C
Section: (none)
Explanation

QUESTION 349
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 350
Matt, a security administrator, is receiving reports about several SQL injections and buffer overflows through his company's website. Which of the following would reduce the amount of these attack types?

A. Antivirus
B. Anti-spam
C. Input validation

D. Host based firewalls

Correct Answer: C
Section: (none)
Explanation

QUESTION 351
A new server image is being created and Sara, the security administrator, would like a baseline created for the servers. Which of the following needs to be taken into account for the baseline?

A. Disabling all unnecessary services
B. Enabling all default accounts
C. Disabling all accounts
D. Enabling all default services

Correct Answer: A
Section: (none)
Explanation

QUESTION 352
Pete, a person who appears to be from a delivery company, is holding a stack of boxes. He requests that the door be held open as he enters the office. Which of following attacks has MOST likely taken place? (Select TWO).

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

Correct Answer: AD
Section: (none)
Explanation

QUESTION 353
The Chief Information Officer (CIO) is concerned that passwords may be written down and posted in plain sight. Which of the following would BEST mitigate this risk?

A. Password expiration policy
B. Clean desk policy
C. Enforce greater password complexity
D. Acceptable use policy

Correct Answer: B
Section: (none)
Explanation

QUESTION 354
Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

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

Correct Answer: BD
Section: (none)
Explanation

QUESTION 355
A company is concerned about proprietary information leaving the network via email. Which of the following is the BEST solution to remediate the risk?

A. Block port 25 on the network
B. Deploy a firewall on the e-mail server
C. Filter incoming traffic
D. Filter outgoing traffic

Correct Answer: D
Section: (none)
Explanation

QUESTION 356
Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

A. Employ encryption on all outbound emails containing confidential information.
B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
C. Employ hashing on all outbound emails containing confidential information.
D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

Correct Answer: A
Section: (none)
Explanation

QUESTION 357
A certificate authority takes which of the following actions in PKI?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 358
To ensure the security of a PKI, security technicians should regularly update which of the following, by checking with the CA for newer versions?

A. CRLs
B. Expiration lists
C. Preshared keys
D. Public keys

Correct Answer: A
Section: (none)
Explanation

QUESTION 359
"First Test, First Pass" - www.lead2pass.com 86
CompTIA SY0-301 Exam

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

A. Malicious code on the local system
B. Shoulder surfing
C. Brute force certificate cracking
D. Distributed dictionary attacks

Correct Answer: A
Section: (none)
Explanation

QUESTION 360
An administrator is provided two accounts: one with administrative access but not network services, and the other account with other network services but no administrative access. Which of the following describes this scenario?

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

Correct Answer: A
Section: (none)

Explanation

QUESTION 361
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 362
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 363
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 364
Which of the following is MOST likely to lead to a breach of security in which Matt, an unauthorized employee, accidently views sensitive data?

A. Lack of business continuity plan
B. Lack of logging and auditing access to files
C. Lack of chain of custody procedure
D. Lack of data labeling, handling, and disposal policies

Correct Answer: D
Section: (none)
Explanation

QUESTION 365
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 366
Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 367
The security administrator wants each user to individually decrypt a message but allow anybody to encrypt it. Which of the following MUST be implemented to allow this type of authorization?

A. Use of CA certificate
B. Use of public keys only
C. Use of private keys only
D. Use of public and private keys

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 368
Jane, a user in the company, is in charge of various financial roles but needs to prepare for an upcoming audit. She uses the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 369
Pete, an employee, is granted access to only areas of a network folder needed to perform his job. Which of the following describes this form of access control?

A. Separation of duties
B. Time of day restrictions
C. Implicit deny
D. Least privilege

Correct Answer: D
Section: (none)
Explanation

QUESTION 370
A security administrator notices unusual activity from a default account when reviewing system logs and finds the account has been compromised. After investigating the incident, the administrator determines the account can be disabled to prevent any further incidents because the account was not necessary for any job functions. Which of the following could have prevented this incident?

A. Enhanced password complexity
B. Disabling unnecessary accounts
C. Reviewing centralized logs
D. Disabling unnecessary services

Correct Answer: B
Section: (none)
Explanation

QUESTION 371
A CRL is comprised of:

A. malicious IP addresses.
B. trusted CA's.
C. untrusted private keys.
D. public keys.

Correct Answer: D
Section: (none)
Explanation

QUESTION 372

Which of the following can be implemented to prevent Matt, a user, from connecting a hub or

switch to a single switch port to access network resources with multiple devices? (Select TWO).

A. Subnetting
B. NAC
C. VLAN
D. DMZ
E. Port security

Correct Answer: BE
Section: (none)
Explanation

QUESTION 373
Which of the following devices utilizes behavior heuristics to detect or prevent intrusion into network resources?

A. NIPS
B. VPN concentrators
C. NAT router
D. Flood guard

Correct Answer: A
Section: (none)
Explanation

QUESTION 374
Which of the following may significantly reduce data loss if multiple drives fail at the same time?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 375
Which of the following would MOST likely belong in the DMZ? (Select TWO).

A. Finance servers
B. Backup servers
C. Web servers
D. SMTP gateways
E. Laptops

Correct Answer: CD
Section: (none)
Explanation

QUESTION 376
Which of the following protocols would MOST likely be implemented if Pete, a user, wants to transfer files reliably from one location to another?

A. SNMP
B. SSH
C. ICMP
"First Test, First Pass" - www.lead2pass.com 90
CompTIA SY0-301 Exam
D. SFTP

Correct Answer: D
Section: (none)
Explanation

QUESTION 377
A server containing critical data will cost the company $200/hour if it were to be unavailable due to DoS attacks. The security administrator expects the server to become unavailable for a total of two days next year. Which of the following is true about the ALE?

A. The ALE is $48.
B. The ALE is $400.
C. The ALE is $4,800.
D. The ALE is $9,600.

Correct Answer: D
Section: (none)
Explanation

QUESTION 378
Jane, a user, installs software downloaded from a trusted website. The installed software causes unwanted pop-ups for pharmaceuticals. Which of the following BEST describes the type of threat?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 379
Sara, a security administrator, notices a number of ports being scanned on the perimeter firewall. At first the scanning appears random, but after monitoring the logs for 30 minutes, she determines that the whole port range is being scanned and all TCP flags are being turned on. Which of the following BEST describes this

type of threat?

A. Smurf attack
B. X-Mas attack
C. Spoofing
D. Malicious insider threat

Correct Answer: B
Section: (none)
Explanation

QUESTION 380
The Chief Information Officer (CIO) receives a call from an individual who states they are from the IT department. The caller wants to know the CIOs ID and password to validate their account as part of a yearly account revalidation process. Which of the following BEST describes this scenario?

A. Spam
B. Hoax
C. Spoofing

D. Vishing

Correct Answer: D
Section: (none)
Explanation

QUESTION 381
To reduce an organization's risk exposure by verifying compliance with company policy, which of the following should be performed periodically?

A. Qualitative analysis
B. Quantitative analysis
C. Routine audits
D. Incident management

Correct Answer: C
Section: (none)
Explanation

QUESTION 382
A buffer overflow can result in which of the following attack types?

A. DNS poisoning
B. Zero-day
C. Privilege escalation
D. ARP poisoning

Correct Answer: C
Section: (none)
Explanation

QUESTION 383
Which of the following is an authentication service that uses UDP as a transport medium?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 384
Which of the following is true concerning WEP security?

A. WEP keys are transmitted in plain text.
B. The WEP key initialization process is flawed.
C. The pre-shared WEP keys can be cracked with rainbow tables.
D. WEP uses the weak RC4 cipher.

Correct Answer: B
Section: (none)
Explanation

QUESTION 385
Matt, a security administrator, wants to secure VoIP traffic on the internal network from eavesdropping. Which of the following would MOST likely be used?

A. SSL
B. SSH
C. QoS
D. IPSec

Correct Answer: D
Section: (none)
Explanation

QUESTION 386
Pete works for a subsidiary company that processes secure transactions for the parent company. Which of the following can be employed to ensure the parent company has access to the subsidiary's encrypted data in an emergency?

A. Trust model
B. Public key infrastructure
C. Symmetrical key encryption
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

QUESTION 387
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

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

Correct Answer: CF
Section: (none)
Explanation

QUESTION 388
Which of the following social engineering attacks is meant for a high-ranking corporate employee?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 389
Which of the following is an advantage of using group policy to redirect users' local folders to networked drives in regards to data loss prevention?

A. Sensitive data is not stored on a local computer.
B. Users can track their data for unauthorized revisions.

C. Incremental back-ups are stored locally for easy access.
D. The users are more aware of where their data is stored.

Correct Answer: A
Section: (none)
Explanation

QUESTION 390
In the case of laptop theft, which of the following is the BEST action to take to prevent data theft?

A. Use a third-party hard drive encryption product.
B. Install the operating system on a non-default partition letter.
C. Set a BIOS password that must be entered upon system boot.
D. Enforce a strict complex operating system password.

Correct Answer: A
Section: (none)
Explanation

QUESTION 391
Pete, a security administrator, has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

A. Internet networks can be accessed via personally-owned computers.
B. Data can only be stored on local workstations.
C. Wi-Fi networks should use WEP encryption by default.
D. Only USB devices supporting encryption are to be used.

Correct Answer: D
Section: (none)
Explanation

QUESTION 392
Sara, a security administrator, needs to implement the equivalent of a DMZ at the datacenter entrance. Which of the following must she implement?

A. Video surveillance
B. Mantrap
C. Access list
D. Alarm

Correct Answer: B
Section: (none)
Explanation

QUESTION 393
Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 394
Sara, a senior programmer for an application at a software development company, has also assumed an auditing role within the same company. She will be assessing the security of the application. Which of the following will she be performing?

A. Blue box testing
B. Gray box testing
C. Black box testing
D. White box testing

Correct Answer: D
Section: (none)
Explanation

QUESTION 395
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 396
Mike, a security analyst, is looking to reduce the number of phishing emails received by employees. Which of the following solutions helps prevent this from occurring?

A. HIDS
B. NIDS
C. Antivirus
D. Spam filter

Correct Answer: D
Section: (none)
Explanation

QUESTION 397
Which of the following BEST describes a directory traversal attack?

A. A malicious user can insert a known pattern of symbols in a URL to access a file in another section of the directory.
B. A malicious user can change permissions or lock out user access from a webroot directory or subdirectories.
C. A malicious user can delete a file or directory in the webroot directory or subdirectories.
D. A malicious user can redirect a user to another website across the Internet.

Correct Answer: A
Section: (none)
Explanation

QUESTION 398
In her morning review of new vendor patches, Jane has identified an exploit that is marked as critical. Which of the following is the BEST course of action?

A. Jane should wait seven days before testing the patch to ensure that the vendor does not issue an updated version, which would require reapplying the patch.
B. Jane should download the patch and install it to her workstation to test whether it will be able to be applied to all workstations in the environment.
C. Jane should alert the risk management department to document the patch and add it to the next monthly patch deployment cycle.
D. Jane should download the patch to the test network, apply it to affected systems, and evaluate the results on the test systems.

Correct Answer: D
Section: (none)
Explanation

QUESTION 399
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 400
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 401
Pete, a security administrator, is working with Jane, a network administrator, to securely design a network at a new location. The new location will have three departments which should be isolated from each other to maintain confidentiality. Which of the following design elements should Pete implement to meet this goal?

A. VLANs
B. Port security
C. VPNs
D. Flood guards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 96
CompTIA SY0-301 Exam

QUESTION 402
Sara, a security administrator, is configuring a new firewall. She has entered statements into the firewall configuration as follows:

Allow all Web traffic
Deny all Telnet traffic
Allow all SSH traffic

Mike, a user on the network, tries unsuccessfully to use RDP to connect to his work computer at home. Which of the following principles BEST explains why Mike's attempt to connect is not successful?

A. Explicit deny
B. Loop protection
C. Implicit deny
D. Implicit permit

Correct Answer: C
Section: (none)
Explanation

QUESTION 403
Jane, a security administrator, notices that a program has crashed. Which of the following logs should Jane check?

A. Access log
B. Firewall log
C. Audit log
D. Application log

Correct Answer: D
Section: (none)
Explanation

QUESTION 404
A process in which the functionality of an application is tested with some knowledge of the internal mechanisms of the application is known as:

A. white hat testing.
B. black box testing.
C. black hat testing.
D. gray box testing.

Correct Answer: D
Section: (none)
Explanation

QUESTION 405
Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8
"First Test, First Pass" - www.lead2pass.com 97
CompTIA SY0-301 Exam

Correct Answer: B
Section: (none)
Explanation

QUESTION 406
Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

A. Retention of user keys
B. Increased logging on access attempts
C. Retention of user directories and files
D. Access to quarantined files

Correct Answer: A
Section: (none)
Explanation

QUESTION 407
Which RAID level is LEAST suitable for disaster recovery plans?

A. 0
B. 1
C. 5
D. 6

Correct Answer: A
Section: (none)

Explanation

QUESTION 408
Which of the following security architecture elements also has sniffer functionality? (Select TWO).

A. HSM
B. IPS
C. SSL accelerator
D. WAP
E. IDS

Correct Answer: BE
Section: (none)
Explanation

QUESTION 409
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 410
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

QUESTION 411
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 412
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

Correct Answer: D
Section: (none)
Explanation

QUESTION 413
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 414
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 415
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 416
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 417
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 418
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

Explanation/Reference:

QUESTION 419
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 420
Sara, an employee, unintentionally downloads malware that exploits a known vulnerability. Which of the following needs to be enforced to keep this incident from recurring in the future?

A. Input validation
B. Active pop-up blocker
C. Application hardening and error validation
D. Patch management

Correct Answer: D
Section: (none)
Explanation

QUESTION 421
Which of the following is being used when a message is buried within the pixels of an image?

A. Steganography
B. Block cipher
C. Encryption
D. Hashing

Correct Answer: A
Section: (none)
Explanation

QUESTION 422
Elliptic curve cryptography: (Select TWO)

A. is used in both symmetric and asymmetric encryption.
B. is used mostly in symmetric encryption.
C. is mostly used in embedded devices.
D. produces higher strength encryption with shorter keys.
E. is mostly used in hashing algorithms.

Correct Answer: CD
Section: (none)
Explanation

QUESTION 423
Which of the following would an antivirus company use to efficiently capture and analyze new and unknown malicious attacks?

A. Fuzzer
B. IDS
C. Proxy
"First Test, First Pass" - www.lead2pass.com 101
CompTIA SY0-301 Exam
D. Honeynet

Correct Answer: D
Section: (none)
Explanation

QUESTION 424
Which of the following is used to translate a public IP to a private IP?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 425
Why is it important for a penetration tester to have established an agreement with management as to which systems and processes are allowed to be tested?

A. Penetration test results are posted publicly, and some systems tested may contain corporate secrets.
B. Penetration testers always need to have a comprehensive list of servers, operating systems, IP subnets, and department personnel prior to ensure a complete test.
C. Having an agreement allows the penetration tester to look for other systems out of scope and test them for threats against the in-scope systems.
D. Some exploits when tested can crash or corrupt a system causing downtime or data loss.

Correct Answer: D
Section: (none)
Explanation

QUESTION 426
An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame. Which of the following strategies would the administrator MOST likely implement?

A. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day

D. Differential backups on the weekend and full backups every day

Correct Answer: A
Section: (none)
Explanation

QUESTION 427
Which of the following can be used in code signing?

A. AES
B. RC4
C. GPG
D. CHAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 102
CompTIA SY0-301 Exam

QUESTION 428
Sara, an administrator, disables the beacon function of an access point. Which of the following is accomplished by this?

A. The AP stops broadcasting radio frequencies.
B. The SSID is not broadcasted by the AP.
C. The AP presence is undetectable by wireless sniffers.
D. Wireless clients are now required to use 2.4 GHz.

Correct Answer: B
Section: (none)
Explanation

QUESTION 429
Jane, an administrator, needs to transfer DNS zone files from outside of the corporate network. Which of the following protocols must be used?

A. TCP
B. ICMP
C. UDP
D. IP

Correct Answer: A
Section: (none)
Explanation

QUESTION 430
Common access cards use which of the following authentication models?

A. PKI
B. XTACACS
C. RADIUS
D. TACACS

Correct Answer: A
Section: (none)
Explanation

QUESTION 431
Which of the following does a second authentication requirement mitigate when accessing privileged areas of a website, such as password changes or user profile changes?

A. Cross-site scripting
B. Cookie stealing
C. Packet sniffing
D. Transitive access

Correct Answer: B
Section: (none)
Explanation

QUESTION 432
Which of the following should Sara, a security technician, educate users about when accessing the company wireless network?

A. IV attacks
B. Vishing
C. Rogue access points
D. Hoaxes

Correct Answer: C
Section: (none)
Explanation

QUESTION 433
Pete, a security technician, has implemented data loss prevention on a company laptop. Which of the following does this protect against?

A. Connecting the company laptop to external data networks
B. Use of USB drives for legitimate operational purposes
C. Use of unencrypted USB drives for gray box testing
D. Removal of company information without authorization

Correct Answer: D
Section: (none)
Explanation

QUESTION 434
Sara, an IT security technician, needs to be able to identify who is in possession of a stolen laptop. Which of the following BEST addresses her need?

A. Remote sanitization
B. Remote wipe
C. GPS tracking
D. Traceroute

Correct Answer: C
Section: (none)
Explanation

QUESTION 435
Which of the following will allow Sara, an IT security technician, to effectively identify a zero-day attack on her systems?

A. Anti-malware
B. Antivirus signatures
C. Host software baseline
D. Virtualization

Correct Answer: C
Section: (none)
Explanation

QUESTION 436
Mike, an IT security technician, needs to recommend an authentication mechanism which has a high probability of correctly identifying a user. Which of the following BEST meets this need?

A. Separation of duties
B. Biometrics
C. Passwords
D. Access control list

Correct Answer: B
Section: (none)
Explanation

QUESTION 437
Jane receives a spreadsheet via email and double clicks the attachment executing another program inside the spreadsheet. Which of the following types of malware was executed?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 438
Which of the following ports does DNS operate on, by default?

A. 23
B. 53
C. 137
D. 443

Correct Answer: B
Section: (none)
Explanation

QUESTION 439
Pete, the system administrator, is concerned about unauthorized access at all entrances into the building. PIN pad readers have been installed, but users have developed the habit of holding the door for others behind them. Which of the following would BEST prevent this?

A. Install mantraps at every unmanned entrance.
B. Replace the PIN pad readers with card readers.
C. Implement video and audio surveillance equipment.
D. Require users to sign conduct policies forbidding these actions.

Correct Answer: A
Section: (none)
Explanation

QUESTION 440
Which of the following is a MAIN objective of implementing a clean desk user policy?

A. Coax users into accepting cloud computing as a viable option.
B. Enforce notions that other users cannot be trusted.
C. Verify that user accounts are strong and complex.
D. Ensure that no sensitive data is left unsupervised.

Correct Answer: D
Section: (none)
Explanation

QUESTION 441
Jane, a network administrator, has configured a 48-port switch to isolate four different departments. Which of the following has Jane MOST likely configured on the switch?

A. NAC

B. 802.1x
C. VLAN
D. DMZ

Correct Answer: C
Section: (none)
Explanation

QUESTION 442
A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 443
Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 444
Which of the following BEST describes a SQL Injection attack?

A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
B. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
D. 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.

Correct Answer: A
Section: (none)
Explanation

QUESTION 445
Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key
B. Asymmetric key
C. Whole disk encryption
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

QUESTION 446
A password history value of three means which of the following?

A. Three different passwords are used before one can be reused.
B. A password cannot be reused once changed for three years.
C. After three hours a password must be re-entered to continue.
D. The server stores passwords in the database for three days.

Correct Answer: A
Section: (none)
Explanation

QUESTION 447
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 448
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 449
In regards to secure coding practices, why is input validation important?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 107
CompTIA SY0-301 Exam

QUESTION 450
A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 451
If Pete, a security administrator, wants to ensure that certain users can only gain access to the system during their respective shifts, which of the following best practices would he implement?

A. Separation of duties
B. Time of day restrictions
C. Implicit deny rule
D. Least privilege

Correct Answer: B
Section: (none)
Explanation

QUESTION 452
Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access?

A. Registration
B. CA

C. CRL
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

QUESTION 453
Which of the following application security testing techniques is implemented when an automated system generates random input data?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 454
Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

A. Cognitive password

B. Password sniffing
C. Brute force
D. Social engineering

Correct Answer: C
Section: (none)
Explanation

QUESTION 455
Which of the following BEST describes a protective countermeasure for SQL injection?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 456
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 457
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 458
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 109
CompTIA SY0-301 Exam

QUESTION 459
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 460
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 461
Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.125
B. 10.4.4.158
C. 10.4.4.165
D. 10.4.4.189
E. 10.4.4.199

Correct Answer: CD
Section: (none)
Explanation

QUESTION 462
Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 463
Developers currently have access to update production servers without going through an approval

process. Which of the following strategies would BEST mitigate this risk?

A. Incident management

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 464
Which of the following is a difference between TFTP and FTP?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 465
Which of the following defines when Pete, an attacker, attempts to monitor wireless traffic in order to perform malicious activities?

A. XSS
B. SQL injection
C. Directory traversal
D. Packet sniffing

Correct Answer: D
Section: (none)
Explanation

QUESTION 466
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 467
Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec

B. Full disk encryption
C. 802.1x
D. PKI
"First Test, First Pass" - www.lead2pass.com 111
CompTIA SY0-301 Exam

Correct Answer: A
Section: (none)
Explanation

QUESTION 468
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 469
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 470
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 471
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 112
CompTIA SY0-301 Exam

QUESTION 472
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 473
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 474
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 475
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 476
A marketing employee requests read and write permissions to the finance department's folders. The security administrator partially denies this request and only gives the marketing employee read-only permissions. This is an example of which of the following?

A. Job rotation
B. Separation of duties
C. Least privilege
D. Change management

Correct Answer: C
Section: (none)
Explanation

QUESTION 477
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 478
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 479
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 480
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 481
Which of the following pseudocodes can be used to handle program exceptions?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 482

Jane, an administrator, hears reports of circles being drawn in the parking lot. Because the symbols fall within range of the company's wireless AP, the MOST likely concern is:

A. that someone has used war chalking to help others access the company's network.
B. that the symbols indicate the presence of an evil twin of a legitimate AP.
C. that someone is planning to install an AP where the symbols are, to cause interference.
D. that a rogue access point has been installed within range of the symbols.

Correct Answer: A
Section: (none)
Explanation

QUESTION 483
Enforcing data encryption of removable media ensures that the:

A. lost media cannot easily be compromised.
B. media can be identified.
C. location of the media is known at all times.
D. identification of the user is non-repudiated.

Correct Answer: A
Section: (none)
Explanation

QUESTION 484
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 485
"First Test, First Pass" - www.lead2pass.com 115
CompTIA SY0-301 Exam

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

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 486
Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 487
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 488
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 489
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 490
Which of the following application attacks is used to gain access to SEH?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 491
Jane, a security technician, has been tasked with preventing contractor staff from logging into the company network after business hours. Which of the following BEST allows her to accomplish this?

A. Time of day restrictions
B. Access control list
C. Personal identity verification
D. Mandatory vacations

Correct Answer: A
Section: (none)
Explanation

QUESTION 492
Which of the following can be implemented on a lost mobile device to help recover it?

A. Remote sanitization
B. GPS tracking
C. Voice encryption
D. Patch management

Correct Answer: B
Section: (none)
Explanation

QUESTION 493
Jane, a security analyst, wants to ensure that data is being stored encrypted, in the event that a corporate laptop is stolen. Which of the following encryption types will accomplish her goal?

A. IPSec
B. Secure socket layer
C. Whole disk
D. Transport layer security

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 117
CompTIA SY0-301 Exam

QUESTION 494
Sara, the Chief Executive Officer (CEO) of a corporation, wishes to receive her corporate email and file attachments on her corporate mobile computing device. If the device is lost or stolen, the BEST security measure to ensure that sensitive information is not comprised would be:

A. to immediately file a police report and insurance report.
B. the ability to remotely wipe the device to remove the data.
C. to immediately issue a replacement device and restore data from the last backup.
D. to turn on remote GPS tracking to find the device and track its movements.

Correct Answer: B
Section: (none)
Explanation

QUESTION 495
Which of the following protocols allows for secure transfer of files? (Select TWO).

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

Correct Answer: CD
Section: (none)
Explanation

QUESTION 496
Users at a corporation are unable to login using the directory access server at certain times of the day. Which of the following concepts BEST describes this lack of access?

A. Mandatory access control
B. Least privilege
C. Time of day restrictions
D. Discretionary access control

Correct Answer: C
Section: (none)
Explanation

QUESTION 497
During a penetration test from the Internet, Jane, the system administrator, was able to establish a

connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

A. 21
B. 22
C. 23
D. 69
E. 3389
F. SSH
G. Terminal services
H. Rlogin
I. Rsync
J. Telnet
"First Test, First Pass" - www.lead2pass.com 118
CompTIA SY0-301 Exam

Correct Answer: BCFJ
Section: (none)
Explanation

QUESTION 498
Matt, an IT security technician, needs to create a way to recover lost or stolen company devices. Which of the following BEST meets this need?

A. Locking cabinets
B. GPS tracking
C. Safe
D. Firewalls

Correct Answer: B
Section: (none)
Explanation

QUESTION 499
Which of the following is the MOST specific plan for various problems that can arise within a system?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 500
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs

B. Mantrap
C. Video surveillance
D. HVAC

Correct Answer: B
Section: (none)
Explanation

QUESTION 501
Which of the following fire suppression systems is MOST likely used in a datacenter?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 502
A security administrator has installed a new KDC for the corporate environment. Which of the

following authentication protocols is the security administrator planning to implement across the organization?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 503
While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 504
Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 505
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 506
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the

network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 507
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 508
Which of the following can be used to discover if a security attack is occurring on a web server?

A. Creating a new baseline
B. Disable unused accounts
C. Implementing full disk encryption
D. Monitoring access logs

Correct Answer: D
Section: (none)
Explanation

QUESTION 509
Jane, the CEO, receives an email wanting her to clink on a link to change her username and password. Which of the following attacks has she just received?

A. Hoaxes
B. Whaling
C. Bluejacking
D. Vishing

Correct Answer: B
Section: (none)
Explanation

QUESTION 510
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 511
Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is $300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 512
Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 513
Which of the following does full disk encryption prevent?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 514
Which of the following can be implemented with multiple bit strength?

A. AES
B. DES
C. SHA-1

D. MD5

E. MD4

Correct Answer: A
Section: (none)
Explanation

QUESTION 515
Pete, the system administrator, has instituted a policy banning personal digital music and video players from the company premises. Which of the following would be the BEST reason for such a policy?

A. The company would be legally liable for any personal device that is lost on its premises.
B. It is difficult to verify ownership of offline device's digital rights management and ownership.
C. The media players may act as distractions during work hours and adversely affect user productivity.
D. If connected to a computer, unknown malware may be introduced into the environment.

Correct Answer: D
Section: (none)
Explanation

QUESTION 516
Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 517
Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 518
Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

A. Authentication server
B. Server certificate
C. Key length
"First Test, First Pass" - www.lead2pass.com 123
CompTIA SY0-301 Exam
D. EAP method

Correct Answer: C
Section: (none)
Explanation

QUESTION 519
Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 520
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 521
Layer 7 devices used to prevent specific types of html tags are called:

A. firewalls.
B. content filters.
C. routers.
D. NIDS.

Correct Answer: B
Section: (none)
Explanation

QUESTION 522
Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
"First Test, First Pass" - www.lead2pass.com 124
CompTIA SY0-301 Exam

QUESTION 523
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 524
In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 525
Which of the following devices is typically used to provide protection at the edge of the network attack surface?

A. Firewall
B. Router
C. Switch
D. VPN concentrator

Correct Answer: A
Section: (none)
Explanation

QUESTION 526
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 527
A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks. Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.
B. The switch has several VLANs configured on it.
C. The sub-interfaces are configured for VoIP traffic.
D. The sub-interfaces each implement quality of service.

Correct Answer: B
Section: (none)
Explanation

QUESTION 528
Digital Signatures provide which of the following?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 529
-- Exhibit --
-- Exhibit --

Use the exhibit button to show a video of an attack. Which of the following BEST describes the type of attack that is occurring?

A. Smurf Attack
B. Man in the middle
C. Backdoor
D. Replay
E. Spear Phishing
F. Xmas Attack
G. Blue Jacking
H. Ping of Death

Correct Answer: A
Section: (none)
Explanation

QUESTION 530
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 531
An administrator might choose to implement a honeypot in order to:

A. provide load balancing for network switches.
B. distract potential intruders away from critical systems.
C. establish a redundant server in case of a disaster.
D. monitor any incoming connections from the Internet.

Correct Answer: B
Section: (none)
Explanation

QUESTION 532
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 533
A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. logic bomb.
B. backdoor.
C. adware application.
D. rootkit.

Correct Answer: B
Section: (none)
Explanation

QUESTION 534
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 535
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

A. RC4
B. 3DES
C. AES
D. MD5

E. PGP
F. Blowfish

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

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

Technical Assistance Center: technology@lead2pass.com

Any problems about IT certification or our products, you could rely upon us, we will give you satisfactory answers in 24 hours.

Our Official: http://www.lead2pass.com