

## SY0-301\_formatted

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



<http://www.gratisexam.com/>

CompTIA SY0-301



CompTIA Security+ Certification 2011

Version: 11.2  
CompTIA SY0-301 Exam

Topic 1, Volume A

## Exam A

### QUESTION 1

Which of the following is an example of a false negative?

- A. The IDS does not identify a buffer overflow
- B. Anti-virus identifies a benign application as malware.
- C. Anti-virus protection interferes with the normal operation of an application.
- D. A user account is locked out after the user mistypes the password too many times.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 2

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 3

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 2  
CompTIA SY0-301 Exam

### QUESTION 4

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

- A. X-Mas attack

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 5

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



<http://www.gratisexam.com/>

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 6

Which of the following accurately describes the STRONGEST multifactor authentication?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 3  
CompTIA SY0-301 Exam

#### QUESTION 7

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 8**

A company is performing internal security audits after a recent exploitation on one of their proprietary applications. Sara, the security auditor, is given the workstation with limited documentation regarding the application installed for the audit. Which of the following types of testing methods is this?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 9**

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

- A. Active fingerprinting
  - B. Passive finger printing
  - C. Protocol analyzing
  - D. Network enumerating
- "Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 4  
CompTIA SY0-301 Exam

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 10**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 11**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 12**

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**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 5  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 13**

The fundamental information security principals include confidentiality, availability and which of the following?

- A. The ability to secure data against unauthorized disclosure to external sources
- B. The capacity of a system to resist unauthorized changes to stored information
- C. The confidence with which a system can attest to the identity of a user
- D. The characteristic of a system to provide uninterrupted service to authorized users

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 14**

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

- A. Continuity of operations
- B. Input validation
- C. Single point of failure
- D. Single sign on

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 15**

Social networking sites are used daily by the marketing team for promotional purposes. However, confidential company information, including product pictures and potential partnerships, have been inadvertently exposed to the public by dozens of employees using social networking sites. Which of following is the BEST response to mitigate this threat with minimal company disruption?

- A. Mandate additional security awareness training for all employees.
- B. Report each employee to Human Resources for termination for violation of security policies
- C. Implement a data loss prevention program to filter email.
- D. Block access to social networking sites from the corporate network "Pass Any Exam. Any Time." -  
www.actualtests.com 6  
CompTIA SY0-301 Exam

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 16**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 17**

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

- A. NIPS

- B. NIDS
- C. ACL
- D. Antivirus

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 18**

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

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 7  
CompTIA SY0-301 Exam

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 19**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 20**

Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

- A. Switches
- B. Protocol analyzers
- C. Routers
- D. Web security gateways

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 21**

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

- A. Phishing
- B. Shoulder surfing
- C. Impersonation  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 8  
CompTIA SY0-301 Exam
- D. Tailgating

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 22**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 23**

Which of the following would Pete, a security administrator, change to limit how far a wireless signal will travel?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 24**

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

- A. TCP 21  
"Pass Any Exam. Any Time." - www.actualtests.com 9  
CompTIA SY0-301 Exam
- B. UDP22
- C. TCP 23
- D. UDP 53

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 25**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 26**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 27**

Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

"Pass Any Exam. Any Time." - www.actualtests.com 10  
CompTIA SY0-301 Exam

- A. 21
- B. 25
- C. 80
- D. 3389

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 28**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 29**

Which of the following is where an unauthorized device is found allowing access to a network?

- A. Bluesnarfing
- B. Rogue access point
- C. Honeypot
- D. IV attack

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 30**

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

"Pass Any Exam. Any Time." - www.actualtests.com 11  
CompTIA SY0-301 Exam

- A. Account expiration
- B. Account lockout

- C. Password complexity
- D. Password length

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 31**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 32**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 33**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 12

CompTIA SY0-301 Exam

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 34**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 35**

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**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 13

CompTIA SY0-301 Exam

**QUESTION 36**

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 37**

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

- A. The DES algorithm is run three consecutive times against the item being encrypted.
- B. The DES algorithm has been used by three parties: the receiving party, sending party, and server.
- C. The DES algorithm has its key length increased to 256.
- D. The DES algorithm is combined with AES and SHA1.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 38**

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**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 14  
CompTIA SY0-301 Exam

**QUESTION 39**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 40**

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:**

Explanation:

**QUESTION 41**

Which of the following has a default port of 22?

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 15  
CompTIA SY0-301 Exam

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 42**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 43**

The public key is used to perform which of the following? (Select THREE).

- A. Validate the CRL
- B. Validate the identity of an email sender

- C. Encrypt messages
- D. Perform key recovery
- E. Decrypt messages
- F. Perform key escrow

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 44**

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

- A. Full disk
  - B. Individual files
  - C. Database
  - D. Partial disk
- "Pass Any Exam. Any Time." - www.actualtests.com 16  
CompTIA SY0-301 Exam

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 45**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 46**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 47**

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 "Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 17 CompTIA SY0-301 Exam 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**

**Explanation/Reference:**

Explanation:

**QUESTION 48**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 49**

Which of the following BEST describes a denial of service attack?

- A. Sara, the attacker, attempts to have the receiving server run a payload using programming commonly found on web servers.
- B. Sara, the attacker, overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
- C. Sara, the attacker, overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.
- D. Sara, the attacker, attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.

**Correct Answer: B**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 50**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 18

CompTIA SY0-301 Exam

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 51**

Matt, a server administrator, sets up database forms based on security rating levels. If a user has the lowest security rating then the database automatically determines what access that user has. Which of the following access control methods does this describe?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 52**

Which of the following is a best practice when securing a switch from physical access?

- A. Disable unnecessary accounts
- B. Print baseline configuration
- C. Enable access lists
- D. Disable unused ports

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 53**

"Pass Any Exam. Any Time." - www.actualtests.com 19

CompTIA SY0-301 Exam

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 54**

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 55**

Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

- A. Account expiration
- B. Password complexity
- C. Account lockout
- D. Dual factor authentication

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 56**

"Pass Any Exam. Any Time." - www.actualtests.com 20

CompTIA SY0-301 Exam

Jane, an IT security technician working at a bank, has implemented encryption between two locations. Which of the following security concepts BEST exemplifies the protection provided by this example?

- A. Integrity
- B. Confidentiality
- C. Cost
- D. Availability

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 57**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 58**

Which of the following should Pete, an administrator, use to verify the integrity of a downloaded file?

- A. CRL
- B. CSR
- C. AES
- D. MD5

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 59**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 21

CompTIA SY0-301 Exam

While Sara is logging into the server from her workstation, she notices Pete watching her enter the username and password. Which of the following social engineering attacks is Pete executing?

- A. Impersonation
- B. Tailgating
- C. Piggybacking
- D. Shoulder surfing

**Correct Answer:** D

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 60**

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

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

**Correct Answer: A**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 61**

The log management system at Company A is inadequate to meet the standards required by their corporate governance team. A new automated log management system has been put in place.

This is an example of which of the following?

- A. Data integrity measurement
- B. Network traffic analysis
- C. Risk acceptance process
- D. Continuous monitoring

**Correct Answer: D**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 62**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 22

CompTIA SY0-301 Exam

Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

- A. Trojan virus
- B. Botnet
- C. Worm outbreak
- D. Logic bomb

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 63**

Which of the following should Sara, a security technician, perform as the FIRST step when creating a disaster recovery plan for a mission critical accounting system?

- A. Implementing redundant systems
- B. Removal of single points of failure
- C. Succession planning
- D. Business impact assessment

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 64**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 65**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 23

CompTIA SY0-301 Exam

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 66**

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

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

- C. Take hashes of the employee's workstation.
- D. Notify security to identify employee's whereabouts.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 67**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 68**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 24

CompTIA SY0-301 Exam

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

- A. Clustering
- B. Virtualization
- C. RAID
- D. Cold site

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 69**

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

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

**Correct Answer:** BC

**Section:** (none)

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 70**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 25  
CompTIA SY0-301 Exam

**QUESTION 71**

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****Explanation/Reference:**

Explanation:

**QUESTION 72**

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

- A. Mean time between failures
- B. A warm recovery site
- C. Mean time to restore
- D. A hot recovery site

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 73**

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**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 26  
CompTIA SY0-301 Exam

**QUESTION 74**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 75**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 76**

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



of the following is the MOST likely cause?

- A. The switch needs to have QoS setup correctly.
  - B. Port security is not enabled on the switch.
  - C. VLAN mismatch is occurring.
  - D. The DMZ is not setup correctly
- "Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 27  
CompTIA SY0-301 Exam

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 77**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 78**

Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

- A. Spoofing
- B. Man-in-the-middle
- C. Dictionary
- D. Brute force
- E. Privilege escalation

**Correct Answer: CD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 79**

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

- A. Trust models
- B. CRL

- C. CA  
"Pass Any Exam. Any Time." - www.actualtests.com 28  
CompTIA SY0-301 Exam
- D. Recovery agent

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 80**

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

- A. Port scanner
- B. Telnet
- C. Traceroute
- D. Honeytrap

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 81**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 82**

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

- A. Lightning rods
- B. EMI shielding
- C. Humidity controls
- D. Temperature controls

"Pass Any Exam. Any Time." - www.actualtests.com 29  
CompTIA SY0-301 Exam

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 83**

An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday.

Which of the following attacks does this describe?

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

**Correct Answer: A**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 84**

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

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

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 85**

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

- A. Header manipulation
  - B. Steganography
  - C. Input validation
  - D. Fuzzing
- "Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 30  
CompTIA SY0-301 Exam

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 86**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 87**

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

- A. NTLM tag
- B. LAN MAN hash
- C. MD5 checksum
- D. SHA summary

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 88**

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

- A. Evil twin
- B. Bluesnarfing  
"Pass Any Exam. Any Time." - www.actualtests.com 31  
CompTIA SY0-301 Exam
- C. War chalking
- D. Bluejacking

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 89**

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

- A. Implement mandatory access controls.
- B. Ensure RAID 0 is implemented on servers.

- C. Impose time of day restrictions across all services
- D. Encrypt all confidential data.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 90**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 91**

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

- A. Hot site  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 32  
CompTIA SY0-301 Exam
- B. Remote site
- C. Cold site
- D. Warm site

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 92**

Jane, a user, has reported an increase in email phishing attempts. Which of the following can be implemented to mitigate the attacks?

- A. Anti-spyware
- B. Anti-adware
- C. Anti-virus
- D. Anti-spam

**Correct Answer:** D

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 93**

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

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

**Correct Answer: A**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 94**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 33  
CompTIA SY0-301 Exam

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

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 95**

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**

### **Explanation/Reference:**

Explanation:

**QUESTION 96**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 97**

Which of the following is BEST utilized to actively test security controls on a particular system?

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 34  
CompTIA SY0-301 Exam

- A. Port scanning
- B. Penetration test
- C. Vulnerability scanning
- D. Grey/Gray box

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 98**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 99**

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

- A. Users shall authenticate to the system via a Kerberos enabled authentication server working with an integrated PKI only.

- B. The system shall require users to authenticate to the system with a combination of a password or PIN and a smartcard
- C. The system shall authenticate only authorized users by fingerprint and retina scan.
- D. Users shall possess a combination of 8 digit PINs and fingerprint scanners.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 100**

Which of the following attacks is characterized by Sara attempting to send an email from a Chief

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 35

CompTIA SY0-301 Exam

Information Officer's (CIO's) non-corporate email account to an IT staff member in order to have a password changed?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Topic 2, Volume B

#### **QUESTION 101**

Which of the following should be done before resetting a user's password due to expiration?

- A. Verify the user's domain membership
- B. Verify the user's identity
- C. Advise the user of new policies
- D. Verify the proper group membership

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 102**

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

- A. Shoulder surfing
- B. Whaling



- C. Tailgating
- D. Impersonation

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 36  
CompTIA SY0-301 Exam

#### **QUESTION 103**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 104**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 105**

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

- A. AP isolation
- B. Port forwarding
- C. DMZ
- D. NAT

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 37  
CompTIA SY0-301 Exam

**QUESTION 106**

Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

- A. Rootkit
- B. Logic bomb
- C. Worm
- D. Botnet

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 107**

Hashing algorithms are used to address which of the following?

- A. Confidentiality
- B. Compatibility
- C. Availability
- D. Integrity

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 108**

After setting up a root CA, which of the following can Pete, a security administrator, implement to allow intermediate CAs to handout keys and certificates?

- A. CRL
- B. Spanning tree
- C. Trust model
- D. Key escrow

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 109**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 110**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 111**

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

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

"Pass Any Exam. Any Time." - www.actualtests.com 39

CompTIA SY0-301 Exam

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 112**

Which of the following should be implemented to restrict wireless access to the hardware address of a NIC?

- A. URL filtering
- B. WPA2 and EAP
- C. PEAP and WPA
- D. MAC filtering

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 113**

Which of the following is the purpose of the spanning tree protocol?

- A. Loop protection
- B. Access control lists
- C. Secure device configuration
- D. Implicit deny

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 114**

Sara, the security engineer, has discovered that a breach is in progress on a non-production system of moderate importance. Which of the following should Sara collect FIRST?

- A. Memory dump, ARP cache



<http://www.gratisexam.com/>

- B. Live system image, route table
  - C. Temp files, hosts file
  - D. Offline system image, router logs
- "Pass Any Exam. Any Time." - www.actualtests.com 40  
CompTIA SY0-301 Exam

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 115**

The Chief Information Security Officer (CISO) tells the network administrator that a security company has been hired to perform a penetration test against their network. The security company asks the CISO which type of testing would be most beneficial for them. Which of the following BEST describes what the security company might do during a black box test?

- A. The security company is provided with all network ranges, security devices in place, and logical maps of the network.
- B. The security company is provided with no information about the corporate network or physical locations.
- C. The security company is provided with limited information on the network, including all network diagrams.
- D. The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 116**

While traveling, users need access to an internal company web server that contains proprietary information. Pete, the security administrator, should implement a:

- A. NAC
- B. VLAN
- C. DMZ
- D. RAS

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 117**

Which of the following is used by Matt, a security administrator, to lower the risks associated with

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 41  
CompTIA SY0-301 Exam  
electrostatic discharge, corrosion, and thermal breakdown?

- A. Temperature and humidity controls
- B. Routine audits
- C. Fire suppression and EMI shielding
- D. Hot and cold aisles

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 118**

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

- A. PGP
- B. DES
- C. AES 256
- D. RSA
- E. 3 DES
- F. AES

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 119**

Workers of a small local organization have implemented an off-site location in which the organization can resume operations within 10 business days in the event of a disaster. This type of site is BEST known as which of the following?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 42  
CompTIA SY0-301 Exam

**QUESTION 120**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 121**

Which of the following may cause Jane, the security administrator, to seek an ACL work around?

- A. Zero day exploit
- B. Dumpster diving
- C. Virus outbreak
- D. Tailgating

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 122**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 43  
CompTIA SY0-301 Exam

#### **QUESTION 123**

Which of the following ports would be blocked if Pete, a security administrator, wants to disable FTP?

- A. 21
- B. 23
- C. 25
- D. 110

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 124**

Sara, a security administrator, suspects that a web server may be under attack. The web logs have several entries containing variations of the following entries:

'or 1=1--

or1'=1--

'or1=1'--

Which of the following attacks is MOST likely occurring?

- A. Zero day exploit
- B. Buffer overflow
- C. SQL injection
- D. Man-in-the-middle

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 125**

Which of the following attacks would be used if Sara, a user, is receiving unwanted text messages?

- A. Packet sniffing  
"Pass Any Exam. Any Time." - www.actualtests.com 44  
CompTIA SY0-301 Exam
- B. Bluesnarfing
- C. Smurf attack
- D. Blue jacking

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 126**

Which of the following practices reduces the attack surface of a wireless network? (Select TWO)

- A. Antenna placement
- B. Using TKIP instead on AES
- C. Power-level control
- D. Using WPA2 instead of WPA
- E. Using RADIUS

**Correct Answer: AC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 127**

Which of the following combinations represents multifactor authentication?

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



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 128**

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

- A. Virtualization  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 45  
CompTIA SY0-301 Exam
- B. Patch management
- C. Full disk encryption
- D. Database encryption

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 129**

Matt, a security administrator, is responsible for provisioning role-based user accounts in an enterprise environment. A user has a temporary business need to perform multiple roles within the organization. Which of the following is the BEST solution to allow the user to perform multiple roles?

- A. Create expiring unique user IDs per role
- B. Allow access to an existing user ID
- C. Assign multiple roles to the existing user ID
- D. Create an additional expiring generic user ID

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 130**

An application programmer reports to Sara, the security administrator, that the antivirus software installed on a server is interfering with one of the production HR applications, and requests that antivirus be temporarily turned off. How should Sara respond to this request?

- A. Ask the programmer to replicate the problem in a test environment.
- B. Turn off antivirus, but install a host intrusion prevention system on the server.
- C. Update the server's antivirus and anti-malware definitions from the vendor's site
- D. Turn off antivirus, but turn on the host-based firewall with a deny-all rule set.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 131**

Which of the following allows active exploitation of security vulnerabilities on a system or network

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 46

CompTIA SY0-301 Exam

for the purpose of determining true impact?

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 132**

A packet filtering firewall can protect from which of the following?

- A. SQL injection
- B. Brute force attack
- C. Port scan
- D. DNS poisoning

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 133**

Which of the following can Matt, an administrator, use to ensure the confidentiality of a file when it is being sent over FTP?

- A. WPA2
- B. PGP
- C. MD5
- D. NTLMv2

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 134**

Pete, a user, submitted a form on the Internet but received an unexpected response shown below

"Pass Any Exam. Any Time." - www.actualtests.com 47  
CompTIA SY0-301 Exam  
Server Error in "/" Application

Runtime error in script on asp.net version 2.0

Which of the following controls should be put in place to prevent Pete from learning this information about the web server in the future?

- A. Patch management
- B. Error handling
- C. Fuzzing
- D. Input validation

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 135**

Employees are reporting that they are receiving unusual calls from the help desk for the purpose of verifying their user credentials. Which of the following attack types is occurring?

- A. Vishing
- B. Spear phishing
- C. Phishing
- D. Pharming

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 136**

Sara, a forensic investigator, believes that the system image she was presented with is not the same as the original source. Which of the following should be done to verify whether or not the image has been tampered with?

- A. Compare file sizes from the original with the system image.
- B. Reimage the original source with a read-only tool set to ignore errors.
- C. Compare hashes of the original source and system image.
- D. Compare time stamps from the original with the system image.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - www.actualtests.com 48  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 137**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 138**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 139**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 49  
CompTIA SY0-301 Exam

**QUESTION 140**

Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

- A. NAT

- B. Virtualization
- C. NAC
- D. Subnetting

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 141**

Which of the following would Sara, a security administrator, utilize to identify 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**

**Explanation/Reference:**

Explanation:

**QUESTION 142**

Matt, a security administrator, wants to allow content owners to determine who has access to files. 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**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 50  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 143**

Which of the following commands can Matt, an administrator, use to create a forensically sound hard drive image?

- A. grep
- B. dump
- C. dd
- D. hex

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 144**

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:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 145**

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:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - www.actualtests.com 51  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 146**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 147**

Jane, a security administrator, has completed the imaging process for 20 computers that were deployed. The image contains the operating system and all required software. Which of the following is this an example of?

- A. Implementing configuration hardening
- B. Implementing configuration baseline
- C. Implementing due diligence
- D. Deploying and using a trusted OS

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 148**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 52  
CompTIA SY0-301 Exam

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 149**

Matt, a system administrator, wants to establish a nightly available SQL database. Which of the following would be implemented to eliminate a single point of failure in storage and servers?

- A. RAID 5 and a storage area network
- B. Two striped drives and clustering
- C. Two mirrored drives and clustering
- D. RAID 0 and load balancing

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 150**

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

- A. Password complexity
- B. Password recovery

- C. 30 day password expiration
- D. Account lockout

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 151**

Which of the following malware types is MOST commonly associated with command and control?

- A. Rootkits
- B. Logic bombs
- C. Botnets
- D. Backdoors

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 53  
CompTIA SY0-301 Exam

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 152**

Which of the following security chips does BitLocker utilize?

- A. BIOS
- B. CPU
- C. CMOS
- D. TPM

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 153**

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

- A. LDAP injection
- B. SQL injection
- C. Error and exception handling
- D. Cross-site scripting

**Correct Answer: D**

**Section: (none)**

**Explanation**



**Explanation/Reference:**

Explanation:

**QUESTION 154**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 54  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 155**

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

- A. Interference
- B. War driving
- C. War chalking
- D. War dialing

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 156**

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

- A. Witness statements
- B. Image hashes
- C. Chain of custody
- D. Order of volatility

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 157**

Which of the following policies is implemented in order to minimize data loss or theft?

- A. PII handling
- B. Password policy
- C. Chain of custody
- D. Zero day exploits

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 55  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 158**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 159**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 160**

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

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

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 161**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 162**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 163**

A company notices that there is a flaw in one of their proprietary programs that the company runs in-house. The flaw could cause damage to the HVAC system. Which of the following would the company transfer to an insurance company?

- A. Risk
- B. Threat
- C. Vulnerability

- D. Code review

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 164**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 165**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 166**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 58  
CompTIA SY0-301 Exam

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

**Correct Answer: D**

**Section: (none)**

**Explanation****Explanation/Reference:**

Explanation:

**QUESTION 167**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 168**

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

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

**Correct Answer: ABF**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 169**

Which of the following attacks is manifested as an embedded HTML image object or JavaScript

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 59

CompTIA SY0-301 Exam

image tag in an email?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 170**

Which of the following is a policy that would force all users to organize their areas as well as help in reducing the risk of possible data theft?

- A. Password behaviors
- B. Clean desk policy
- C. Data handling
- D. Data disposal

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 171**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 172**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 60

CompTIA SY0-301 Exam

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 173**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 174**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 175**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 61

CompTIA SY0-301 Exam

Traffic has stopped flowing to and from the company network after the inline IPS hardware failed.

Which of the following has occurred?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 176**

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

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

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 177**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 62  
CompTIA SY0-301 Exam

**QUESTION 178**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 179**

Which of the following multifactor authentication methods uses biometrics?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 180**

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

Sales Department - Read

Marketing Department - Full Control

Inside Sales - Read Write

This is an example of which of the following?

- A. RBAC
  - B. MAC
  - C. RSA
  - D. DAC
- "Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 63  
CompTIA SY0-301 Exam

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 181**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 182**

Which of the following control types is video monitoring?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 183**

Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

- A. Succession planning
  - B. Disaster recovery
  - C. Separation of duty
  - D. Removing single loss expectancy
- "Pass Any Exam. Any Time." - www.actualtests.com 64  
CompTIA SY0-301 Exam

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 184**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 185**

Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential- type authentication method BEST fits these requirements?

- A. EAP-TLS
- B. EAP-FAST
- C. PEAP-CHAP
- D. PEAP-MSCHAPv2

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 186**

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

- A. Install both the private and the public key on the client machine.  
"Pass Any Exam. Any Time." - www.actualtests.com 65  
CompTIA SY0-301 Exam
- B. Install both the private and the public key on the web server.
- C. Install the public key on the web server and the private key on the client machine.
- D. Install the public key on the client machine and the private key on the web server.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 187**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 188**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 189**

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

"Pass Any Exam. Any Time." - www.actualtests.com 66  
CompTIA SY0-301 Exam

- A. Analyze the vulnerability results from the scan.
- B. Mitigate risk and develop a maintenance plan.

- C. Ignore risk and document appropriately to address at a later time.
- D. Transfer risk to web application developers.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 190**

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

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 191**

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

- A. Update the CRL
- B. Change the trust model
- C. Deploy a key escrow
- D. Query the intermediate CA
- E. Deploy a recovery agent
- F. Deploy OCSP

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 192**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 67

CompTIA SY0-301 Exam

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 193**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 194**

A vulnerability has been found in a service that is unnecessary for the corporate environment. Which of the following is the BEST way to mitigate this vulnerability?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 68  
CompTIA SY0-301 Exam

**QUESTION 195**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 196**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 197**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 69  
CompTIA SY0-301 Exam

**QUESTION 198**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 199**

Which of the following is characterized by an attack against a mobile device?

- A. Evil twin

- B. Header manipulation
- C. Blue jacking
- D. Rogue AP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 200**

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

- A. Loop protection
- B. Flood guards
- C. Port security
- D. ACL

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Topic 3, Volume C

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 70  
CompTIA SY0-301 Exam

**QUESTION 201**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 202**

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

- A. Error and exception handling
- B. Application hardening
- C. Application patch management
- D. Cross-site script prevention

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 203**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 71  
CompTIA SY0-301 Exam

**QUESTION 204**

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

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

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 205**

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

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

**Correct Answer:** D

**Section:** (none)



## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 206**

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

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

**Correct Answer: A**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 72  
CompTIA SY0-301 Exam

Explanation:

### **QUESTION 207**

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

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

**Correct Answer: D**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 208**

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

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

**Correct Answer: C**

**Section: (none)**

### **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 209**

Which of the following represents the WEAKEST password?

- A. PaSsWoRd
- B. P@sSWOr&
- C. P@sSW1r&
- D. PassW1rD

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - www.actualtests.com 73  
CompTIA SY0-301 Exam

Explanation:

**QUESTION 210**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 211**

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

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 212**

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

- A. Cable locks

- B. Strong passwords
  - C. Voice encryption
  - D. Remote sanitization
- "Pass Any Exam. Any Time." - www.actualtests.com 74  
CompTIA SY0-301 Exam

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 213**

Matt, a security administrator, wants to configure all the switches and routers in the network in order to security monitor their status. Which of the following protocols would he need to configure on each device?

- A. SMTP
- B. SNMPv3
- C. IPSec
- D. SNMP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 214**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 215**

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 "Pass Any Exam. Any Time." -  
www.actualtests.com 75  
CompTIA SY0-301 Exam
- D. Security alerts will be minimal until adequate traffic is collected

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 216**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 217**

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

- A. Logic bomb
- B. Whaling
- C. Man-in-the-middle
- D. Smurf attack

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 218**

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

- A. Enforce a policy for all users to authentic through a biometric device.
- B. Disable all SSID broadcasting  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 76  
CompTIA SY0-301 Exam
- C. Ensure all access points are running the latest firmware.
- D. Move all access points into public access areas.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 219**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 220**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 221**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 77  
CompTIA SY0-301 Exam

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 222**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 223**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 224**

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

- A. Patch management  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 78  
CompTIA SY0-301 Exam
- B. Application fuzzing
- C. ID badge
- D. Application configuration baseline

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 225**

Which of the following data center 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**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 226**

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

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

**Correct Answer: C**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 227**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 79  
CompTIA SY0-301 Exam

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

**Correct Answer: DF**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

#### **QUESTION 228**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 229**

Which of the following data encryption types will BEST protect data in motion and at rest to a cloud provider?

- A. File encryption
- B. Transport
- C. PKI
- D. SHA-256

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 230**

Which of the following will mitigate the effects of devices in close proximity?

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 80  
CompTIA SY0-301 Exam

- A. EMI shielding
- B. Load balancing
- C. Grounding
- D. Video monitoring

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 231**

A major CA has been compromised and a new patch has been released to make necessary changes on user machines. Which of the following is likely to be updated as a part of this patch?

- A. Recovery agent
- B. CRL
- C. Key escrow
- D. PKI

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 232**

Which of the following uses both a public and private key?

- A. RSA



- B. AES
- C. MD5
- D. SHA

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 233**

Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 81  
CompTIA SY0-301 Exam

- A. Tailgating
- B. Fencing
- C. Screening
- D. Mantrap

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 234**

Symmetric encryption utilizes \_\_\_\_\_. While asymmetric encryption utilizes \_\_\_\_\_.

- A. Public keys, one time
- B. Shared keys, private keys
- C. Private keys, session keys
- D. Private keys, public keys

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 235**

Jane, an administrator, notices that after 2,000 attempts a malicious user was able to compromise an employee's password. Which of the following security controls BEST mitigates this type of external attack? (Select TWO).

- A. Account expiration
- B. IDS
- C. Password complexity
- D. Server logging
- E. Account lockout

F. Proxy server

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 236**

Matt, the network engineer, has been tasked with separating network traffic between virtual

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 82

CompTIA SY0-301 Exam

machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

- A. Virtual switch
- B. NAT
- C. System partitioning
- D. Access-list
- E. Disable spanning tree
- F. VLAN

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 237**

Sara, an IT manager, wants to change the firewall rules to allow RemoteOfficeB to connect to the corporate network using SSH. Which of the following rules would only allow necessary access?

- A. Permit RemoteOfficeB any port 69
- B. Permit RemoteOfficeB any all
- C. Permit RemoteOfficeB any port 22
- D. Permit any corporate port 443

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 238**

Which of the following attacks is characterized by someone following a staff member who is entering a corporate facility?

- A. Evil twin
- B. Tailgating
- C. Shoulder surfing
- D. Impersonation

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 83  
CompTIA SY0-301 Exam

**QUESTION 239**

Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

- A. Two factor authentication
- B. Identification and authorization
- C. Single sign-on
- D. Single factor authentication

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 240**

Jane, a corporate user, is trying to secure her laptop from drive-by download before she leaves for a computer conference. Which of the following should be installed to keep Jane's laptop secure from these attacks?

- A. Full disk encryption
- B. Host based firewall
- C. Antivirus system
- D. Network based firewall

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 241**

Which of the following detection methods may generate an alert when Matt, an employee, accesses a server during non-business hours?

- A. Signature
- B. Time of Day restrictions
- C. Heuristic
- D. Behavioral

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 84  
CompTIA SY0-301 Exam

**QUESTION 242**

Which of the following data is typically left unencrypted in software based full disk encryption?

- A. OS registry
- B. Extended partition
- C. BIOS
- D. MBR

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 243**

Which of the following is an authentication service that uses symmetrical keys and tickets?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 244**

Which of the following application attacks is identified by use of the <SCRIPT> tag?

- A. XSS
- B. Buffer overflow
- C. Directory traversal
- D. Zero day

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 85  
CompTIA SY0-301 Exam

**QUESTION 245**

Jane, a security architect, is working on setting up a secure email solution between internal employees and external customers. Which of the following would BEST meet her goal?

- A. Public key infrastructure
- B. Key escrow
- C. Internal certificate authority
- D. Certificate revocation list

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 246**

Which of the following allows multiple internal IP addresses to be mapped to one specific external IP address?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 247**

Which of the following would Jane, a security administrator, use to encrypt transmissions from streaming video transmissions, keeping in mind that each bit must be encrypted as it comes across the network?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 86  
CompTIA SY0-301 Exam

Explanation:

#### **QUESTION 248**

Matt, a user, finds a flash drive in the parking lot and decides to see what is on it by using his company laptop. A few days later Matt reports his laptop is running slow and is unable to perform simple tasks. The security administrator notices several unauthorized applications have been installed. CPU usage is unusually high, and a collection of screenshots of Matt's recent activity has been transmitted over the network. This is an example of which of the following?

- A. Backdoor
- B. Logic bomb

- C. Rootkit
- D. Spyware

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 249**

Pete, the security administrator, found that several of the company's workstations are infected with a program aimed at stealing users' cookies and reporting them back to the malicious user. Which of the following attack types is the malicious user MOST likely to carry out with this information?

- A. Man-in-the-middle
- B. Session hijacking
- C. Command injection
- D. Trojan infection

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 250**

Sara, a security administrator, is implementing remote management for network infrastructure using SNMP. Which of the following statements is true about SNMP?

- A. Read communities allow write permissions  
"Pass Any Exam. Any Time." - www.actualtests.com 87  
CompTIA SY0-301 Exam
- B. Relays mail based on domain keys and access headers
- C. SNMP communities are encrypted using PKI
- D. Write communities allow both read and write permissions

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 251**

Which of the following mitigation techniques is Pete, a security administrator, MOST likely to implement after the software has been released to the public?

- A. Error and exception handling
- B. Fuzzing
- C. Secure coding
- D. Patch management

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 252**

Which of the following BEST defines risk?

- A. A threat will have a larger impact than anticipated
- B. Remediation of a known vulnerability is cost prohibitive
- C. A degree of probability of loss
- D. A user leaves a system unsecure

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 253**

Companies allowing remote access to internal systems or systems containing sensitive data should provide access using:

- A. dial-up or broadband networks using passwords.  
"Pass Any Exam. Any Time." - www.actualtests.com 88  
CompTIA SY0-301 Exam
- B. wireless networks using WPA encryption.
- C. VPN with two factor authentication.
- D. carrier based encrypted data networks

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 254**

Which of the following is the proper order for incident response?

- A. Detection, preparation, containment, eradication, recovery
- B. Preparation, detection, containment, eradication, recovery
- C. Preparation, detection, recovery, eradication, containment
- D. Detection, containment, eradication, recovery, preparation

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 255**

Which of the following is considered the MOST secure wireless encryption measure to implement?

- A. TKIP
- B. CCMP
- C. WPA2
- D. WEP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 256**

Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

- A. 3DES  
"Pass Any Exam. Any Time." - www.actualtests.com 89  
CompTIA SY0-301 Exam
- B. Blowfish
- C. Serpent
- D. AES256

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 257**

A team is developing a new application with many different screens that users can access. The team decides to simplify access by creating just two internal application roles. One role is granted read-only access to the summary screen. The other role is granted update access to all screens. This simplified access model may have a negative security impact on which of the following?

- A. Remote access
- B. Identity management
- C. Least privilege
- D. Authentication

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 258**

Which of the following would be the BEST choice for attacking a complex password hash?

- A. Man in the middle
- B. Dictionary files
- C. Rainbow tables



D. Brute-force intrusion

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 259**

In order for Pete, a user, to logon to his desktop computer, he must provide his username, password, and use a common access card with a PIN. Which of the following authentication methods is Pete using?

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 90  
CompTIA SY0-301 Exam

A. Single factor

B. Two factor

C. Three factor

D. Four factor

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 260**

Which of the following is a reason why a company might deploy data encryption?

A. To maintain the integrity of the information

B. To keep information confidential

C. To prevent data corruption

D. To prevent backup tape theft

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 261**

Which of the following would Sara, a security administrator, implement to divert and analyze attacks?

A. Protocol analyzer

B. DMZ

C. Port scanner

D. Honeytrap

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 262**

In PKI, the public key is used to:

"Pass Any Exam. Any Time." - www.actualtests.com 91  
CompTIA SY0-301 Exam

- A. decrypt the signature CRC.
- B. decrypt an email message.
- C. encrypt an email message.
- D. encrypt the signature hash.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 263**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 264**

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**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - www.actualtests.com 92  
CompTIA SY0-301 Exam

**QUESTION 265**

The health care department is storing files with names, addresses, and social security numbers on a corporate file server. Matt, the security analyst, comes across this data in an audit. Which of the following has Matt discovered?

- A. Personal identifiable information
- B. Data classification rules
- C. Data disposal procedures
- D. Data handling rules

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 266**

Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

- A. SHA1
- B. MD2
- C. MD4
- D. MD5

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 267**

Which of the following would Jane, a security administrator, use to authenticate remote users into the network?

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 93  
CompTIA SY0-301 Exam

- A. RADIUS
- B. XTACACS
- C. TACACS
- D. ACLs

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 268**

A company wants to implement a policy that helps reduce employee stress and decrease the likelihood of security incidents caused by job dissatisfaction. Which of the following will MOST likely have a positive impact on the employee stress and job satisfaction?

- A. Change management
- B. Mandatory vacations
- C. Due care
- D. Service Level Agreements

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 269**

Pete would like to implement a new tape backup plan for HR to speed up the process of nightly backups on their file systems HR does not make many file alterations on Tuesday through Thursday. Pete does a full backup on Monday and again on Friday. Which of the following should Pete do to speed up the backups Tuesday through Thursday?

- A. Incremental backups Tuesday through Thursday
- B. Full backups Tuesday through Thursday
- C. Differential backups Tuesday through Thursday
- D. Differential backups Tuesday and Wednesday

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 94  
CompTIA SY0-301 Exam

**QUESTION 270**

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**

**Explanation/Reference:**

Explanation:

**QUESTION 271**

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

- A. ECC
- B. RSA

- C. SHA
- D. 3DES

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 272**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 95  
CompTIA SY0-301 Exam

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 273**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 274**

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

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 96

CompTIA SY0-301 Exam

**QUESTION 275**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 276**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 277**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 97

CompTIA SY0-301 Exam

- A. The router ACL matches VPN traffic. The NAC server verifies antivirus signatures are supported and up-to-date.
- B. The NAC server processes the authentication, and then it matches patches and antivirus signatures with its local database.
- C. The access control server connects to the agent on the users' client to set minimal accepted levels of

patching and signatures allowed. The agent creates a token which the router can match for access.

- D. The router sends queries to the access control server; the access control server handles proxy requests to third party patching and antivirus servers.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 278**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 279**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 98  
CompTIA SY0-301 Exam

Explanation:

#### **QUESTION 280**

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

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 281**

Which of the following protocols allows for the LARGEST address space?

- A. IPX
- B. IPv4
- C. IPv6
- D. Appletalk

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 282**

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

- A. RIO analysis  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 99  
CompTIA SY0-301 Exam
- B. Benchmarking
- C. Market analysis
- D. Usability testing

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 283**

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

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 284**

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



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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 285**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 100 CompTIA SY0-301 Exam

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 286**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 287**

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

- A. Full disk encryption
- B. Application isolation
- C. Digital rights management

D. Data execution prevention

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 101 CompTIA SY0-301 Exam

**QUESTION 288**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 289**

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

- A. Mobile device encryption
- B. Full disk encryption
- C. Transport encryption
- D. Database encryption

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 290**

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 102 CompTIA SY0-301 Exam

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 291**

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

- A. VLAN
- B. DIMSSEC
- C. ACL
- D. 802.1X

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 292**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 103 CompTIA SY0-301 Exam

**QUESTION 293**

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

- A. Impersonation
- B. Vishing
- C. Shoulder surfing
- D. Tailgating

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 104



<http://www.gratisexam.com/>