

## CompTIA Exactexams SY0-301 Questions & Answers

Number: SY0-301  
Passing Score: 800  
Time Limit: 120 min  
File Version: 31.4



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



**CompTIA SY0-301 Questions & Answers**

**Exam Name: CompTIA Security+ Certification Exam 2011**

**For Full Set of Questions please visit: <http://www.exact-exams.com/SY0-301-exam.htm>**

## 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:

### QUESTION 4

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:

#### **QUESTION 5**

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 6**

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 7**

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:**

Explanation:

#### QUESTION 8

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 9

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?



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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 10

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 11**

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 12**

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 13**

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:

**QUESTION 14**

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 15**

Which of the following has a default port of 22?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 16**

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 17**

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 18**

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

## **Exam B**

### **QUESTION 1**

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 2**

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 3**

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 4**

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 5**

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 6**

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 7**

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 8**

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 9**

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:

**QUESTION 10**

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 11**

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 12**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 13**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 14**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 15**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 16**

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 17**

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 18**

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 19**

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:

## **Exam C**

### **QUESTION 1**

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 2**

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 3**

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 4**

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 5**

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 6**

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 7**

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:



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

#### QUESTION 8

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 9

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:

#### QUESTION 10

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



**QUESTION 11**

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 12**

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:**

Explanation:

**QUESTION 13**

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 14**

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 15**

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:**

Explanation:

**QUESTION 16**

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:**

Explanation:

**QUESTION 17**

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:

## Exam D

### QUESTION 1

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 2

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:**

Explanation:

### QUESTION 3

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 4

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 5**

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 6**

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 7**

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 8**

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 9**

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

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 10**

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 11**

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

image tag in an email?

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

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 12**

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 13**

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 14**

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 15**

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 16**

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 17**

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:



**QUESTION 18**

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

Sales Department - Read

Marketing Department - Full Control

Inside Sales - Read Write

This is an example of which of the following?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 19**

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 20**

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 21**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 22**

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 23**

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 24**

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 25**

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 26**

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 27**

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 28**

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:

## Exam E

### QUESTION 1

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 2

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:

### QUESTION 3

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 4

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 5**

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 6**

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 7**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 8**

Which of the following describes common concerns when implementing IPS?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 9**

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 10**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 11**

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 12**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 13**

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 14**

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 15**

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

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

**Correct Answer:** DF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 16**

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 17**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 18**

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 19**

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 20**

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 21**

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:

**QUESTION 22**

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 23**

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 24**

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 25**

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 26**

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:

#### **QUESTION 27**

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 28**

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 29**

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 30**

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:**

Explanation:

## Exam F

### QUESTION 1

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 2

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 3

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 4

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 5**

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

- A. 3DES
- B. Blowfish
- C. Serpent
- D. AES256

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 6**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 7**

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 8**

In PKI, the public key is used to:

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 9**

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 10**

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:



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

#### **QUESTION 11**



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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 12**

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:

#### **QUESTION 13**

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 14**

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 15**

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:

**QUESTION 16**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 17**

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 18**

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:**

Explanation:

### **QUESTION 19**

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

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

**Correct Answer: A**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 20**

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

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

**Correct Answer: A**

**Section: (none)**

## **Explanation**

### **Explanation/Reference:**

Explanation:

### **QUESTION 21**

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:

#### **QUESTION 22**

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 23**

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 24**

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:



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