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

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
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 3
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 4
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 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 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 7
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 8
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 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?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Pete, the security administrator, is implementing a web content fitter. Which of the following is the MOST important design consideration in regards to availability?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
When used alone, which of the following controls mitigates the risk of Sara, an attacker, launching an online brute force password attack?

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

Correct Answer: B
Section: (none)
Explanation

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
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 15
Which of the following types of data encryption would Jane, a security administrator, use if MBR and the file systems needed to be included?

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

Correct Answer: A
Section: (none)
Explanation

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
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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. Verity the proper group membership

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Sara, an attacker, calls the company's from desk and tries to gain insider information by providing specific company information to gain the attendant's trust. The front desk immediately alerts the IT department about this incident. This is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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 4
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 5
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
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 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:

QUESTION 8
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:

QUESTION 9
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 10
Which of the following attacks would be used if Sara, a user, is receiving unwanted text messages?

A. Packet sniffing
B. Bluesnarfing
C. Smurf attack
D. Blue jacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
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 12
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 13
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 14
Sara, a forensic invest gator, believes that the system image she was presented with is not the same as the original source. Which of the following should be done to verify whether or not the image has been tampered with?

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

D. Compare time stamps from the original with the system image.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Which of the following would Sara, a security administrator, utilize to identity a weakness within various applications without exploiting that weakness?

A. Protocol analyzer
B. Port scanner
C. Vulnerability scan
D. Penetration test

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Matt, a security administrator, wants to allow content owners to determine who has access to tiles. Which of the following access control types does this describe?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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 18
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 malware types is MOST commonly associated with command and control?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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 3
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 4
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 5
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 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
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 8
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 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
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 11
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 12
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 13
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 14
A company is installing a wireless network in a building that houses several tenants. Which of the following should be considered to make sure none of the other tenants can detect the company's wireless network? (Select TOO).

A. Static IP addresses

B. Wireless encryption
C. MAC filtering
D. Antenna placement
E. Power levels

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Pete is reporting an excessive amount of junk mail on the network email server. Which of the following would ONLY reduce the amount of unauthorized mail?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
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 17
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 18
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 19
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 20
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 21
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 22
The IT Security Department has completed an internal risk assessment and discovered the use of an outdated antivirus definition file. Which of the following is the NEXT step that management should take?

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

Correct Answer: B
Section: (none)
Explanation

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 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 29
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
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 3
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 4
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 5
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 6
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 7
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 8
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 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
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 11
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 12
Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
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 14
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 15
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 16
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 17
Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
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 19
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 20
Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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 22
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 23
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 24
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 25

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 26
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 27
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 28
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 29
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
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 10
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 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
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
Jane, a security technician, needs to develop access controls for the network. In which of the following access control types does a user determine who has access to certain network resources?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 22
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 23
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: