CompTIA aiotestking.com SY0-301 - Jerry

Number: 000-000
Passing Score: 750
Time Limit: 90 min
File Version: 1.0

http://www.gratisexam.com/

Sections

1. Exam A
2. Exam B
3. Exam C
4. Exam D
5. Exam E

Exam A

QUESTION 1
Which of the following elements of PKI are found in a browser's trusted root CA?

A. Private key
B. Symmetric key
C. Recovery key
D. Public key

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 2
DRPs should contain which of the following?

A. Hierarchical list of non-critical personnel
B. Hierarchical list of critical systems
C. Hierarchical access control lists
D. Identification of single points of failure

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 3
Which of the following is specific to a buffer overflow attack?

A. Memory addressing
B. Directory traversal
C. Initial vector
D. Session cookies

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 4
In an 802.11n network, which of the following provides the MOST secure method of both encryption and authorization?

A. WEP with 802.1x
B. WPA Enterprise
C. WPA2-PSK
D. WPA with TKIP

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 5
A security administrator finished taking a forensic image of a computer's memory. Which of the following should the administrator do to ensure image integrity?

A. Run the image through AES128.
B. Run the image through a symmetric encryption algorithm.
C. Compress the image to a password protected archive.
D. Run the image through SHA256.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 6
A security manager believes that too many services are running on a mission critical database server. Which of the following tools might a security analyst use to determine services that are running on the server, without logging into the machine?

GRATIS EXAM
Free Practice Exams
http://www.gratisexam.com/

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

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 7
Which of the following describes software that is often written solely for a specific customer application?

A. Rootkit
B. Hotfix
C. Service pack
D. Patch

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 8
Which of the following hashing techniques is commonly disabled to make password cracking more difficult?

A. NTLM
B. AES
C. OVAL
D. Kerberos

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 9
An administrator wants to ensure that when an employee leaves the company permanently, that the company will have access to their private keys. Which of the following will accomplish this?

A. Store the keys in escrow.
B. Immediately delete the account.
C. Store them in a CRL.
D. Obtain the employee's hardware token.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 10
An administrator wants to block users from accessing a few inappropriate websites as soon as possible. The existing firewall allows blocking by IP address. To achieve this goal the administrator will need to:

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

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 11

Which of the following is a risk associated with a virtual server?

A. If the physical server crashes, all of the local virtual servers go offline immediately.
B. If the physical server crashes, all of the physical servers nearby go offline immediately.
C. If a virtual server crashes, all of the virtual servers go offline immediately.
D. If a virtual server crashes, all of the physical servers go offline immediately.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is the quickest method to create a secure test server for a programmer?

A. Install a network operating system on new equipment.
B. Create a virtual server on existing equipment.
C. Install a network operating system on existing equipment.
D. Create a virtual server on new equipment.

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 13
All of the following require periodic updates to stay accurate EXCEPT:

A. signature based HIDS.
B. pop-up blocker applications.
C. antivirus applications.
D. rootkit detection applications.

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 14
All of the following are where backup tapes should be kept EXCEPT:

A. near a fiber optic cable entrance.
B. near a shared LCD screen.
C. near a power line.
D. near a high end server.

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 15
A single sign-on requires which of the following?

A. Multifactor authentication
B. One-factor authentication
C. A trust model between workstations
D. A unified trust model

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 16
Which of the following allows for a secure connection to be made through a web browser?

A. L2TP
B. SSH
C. SSL
D. HTTP

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 17
Which of the following would allow for secure key exchange over an unsecured network without a pre-shared key?

A. 3DES
B. AES
C. DH-ECC
D. MD5

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 18
Which of the following is a problem MOST often associated with UTP cable?

A. Fuzzing
B. Vampire tap

C. Crosstalk
D. Refraction

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 19
To evaluate the security compliance of a group of servers against best practices, which of the following BEST applies?

A. Get a patch management report.
B. Conduct a penetration test.
C. Run a vulnerability assessment tool.
D. Install a protocol analyzer.

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 20
Which of the following describes the difference between a secure cipher and a secure hash?

A. A hash produces a variable output for any input size, a cipher does not.
B. A cipher produces the same size output for any input size, a hash does not.
C. A cipher can be reversed, a hash cannot
D. A hash can be reversed, a cipher cannot.

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 21
Configuration baselines should be taken at which of the following stages in the deployment of a new system?

A. Before initial configuration.
B. Before loading the OS.
C. After a user logs in.
D. After initial configuration.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 22
Social engineering, password cracking and vulnerability exploitation are examples of which of the following?

A. Vulnerability assessment.
B. Fingerprinting.
C. Penetration testing.
D. Fuzzing.

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 23
Frequent signature updates are required by which of the following security applications? (Select TWO).

A. Antivirus
B. PGP
C. Firewall
D. PKI
E. IDS

Correct Answer: AE
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 24
A flat or simple role-based access control (RBAC) embodies which of the following principles?

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

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 25
A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of 5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in

the call center are paid $90 per hour. If the anti-malware software is purchased, which of the following is the expected net savings?

A. 9000
B. 2,290
C. 2,700
D. 5,000

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 26
A small call center business decided to install an email system to facilitate communications in the office. As part of the upgrade the vendor offered to supply anti-malware software for a cost of 5,000 per year. The IT manager read there was a 90% chance each year that workstations would be compromised if not adequately protected. If workstations are compromised it will take three hours to restore services for the 30 staff. Staff members in the call center are paid $90 per hour. If determining the risk, which of the following is the annual loss expectancy (ALE)?

A. $2,700
B. $9,500
C. $8,100
D. $7,290

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 27
After a system risk assessment was performed it was found that the cost to mitigate the risk was higher than the expected loss if the risk was actualized. In this instance, which of the following is the BEST course of action?

A. Accept the risk.
B. Mitigate the risk.
C. Reject the risk.
D. Run a new risk assessment.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 28
A CEO is concerned about staff browsing inappropriate material on the Internet via HTTPS. It has been suggested that the company purchase a product which could decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing. Which of the following type of attacks is similar to this

product?

A. Replay.
B. Spoofing.
C. TCP/IP hijacking.
D. Man-in-the-middle.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 29
A technician suspects that one of the network cards on the internal LAN is causing a broadcast storm. Which of the following would BEST diagnose which NIC is causing this problem?

A. The NIDS log file.
B. A protocol analyzer.
C. The local security log file.
D. The local firewall log file.

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 30
Which of the following would be BEST to use to apply corporate security settings to a device?

A. A security patch.
B. A security hotfix.
C. An OS service pack.
D. A security template.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 31
Which of the following allows a file to have different security permissions for users that have the same roles or user groups?

A. Mandatory Access Control (MAC)
B. Role-Based Access Control (RBAC)
C. Discretionary Access Control (DAC)
D. Rule-Based Access Control (RBAC)

Correct Answer: C

Section: Exam A
Explanation

Explanation/Reference:

QUESTION 32
Using an asymmetric key cryptography system, where can a technician generate the key pairs?

A. A certificate authority.
B. IETF
C. A key escrow service.
D. A recovery agent.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 33
Which of the following uses a key ring?

A. AES
B. DES
C. PGP
D. RSA

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 34
Which of the following allows a technician to scan for missing patches on a device without actually attempting to exploit the security problem?

A. A vulnerability scanner.
B. Security baselines.
C. A port scanner.
D. Group policy.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 35
When dealing with a 10BASE5 network, which of the following is the MOST likely security risk?

A. An incorrect VLAN.

B. SSID broadcasting.
C. A repeater.
D. A vampire tap.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 36
Which of the following allows for notification when a hacking attempt is discovered?

A. NAT
B. NIDS
C. Netflow
D. Protocol analyzer.

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 37
Which of the following is the MOST recent addition to cryptography?

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

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 38
Which of the following algorithms have the smallest key space?

A. IDEA
B. SHA-1
C. AES
D. DES

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 39
An administrator notices that former temporary employee's accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

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

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is a reason why a company should disable the SSID broadcast of the wireless access points?

A. Rogue access points.
B. War driving.
C. Weak encryption.
D. Session hijacking.

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 41
Antivirus software products detect malware by comparing the characteristics of known instances against which of the following type of file sets?

A. Signature.
B. Text
C. NIDS signature.
D. Dynamic Library.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 42
A user is attempting to receive digitally signed and encrypted email messages from a remote office. Which of the following protocols does the system need to support?

A. SMTP
B. S/MIME

C. ISAKMP
D. IPSec

Correct Answer: B
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is the primary purpose of a CA?

A. LANMAN validation.
B. Encrypt data.
C. Kerberos authentization.
D. Issue private/public keys.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 44
Which of the following type of attacks requires an attacker to sniff the network?

A. Man-in-the-Middle.
B. DDos attack.
C. MAC flooding.
D. DNS poisoning.

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 45
Which of the following can be used as a means for dual-factor authentication?

A. RAS and username/password.
B. RADIUS and L2TP.
C. LDAP and WPA.
D. Iris scan and proximity card.

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 46
Which of the following is the BEST way to reduce the number of accounts a user must maintain?

A. Kerberos
B. CHAP
C. SSO
D. MD5

Correct Answer: C
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 47
Which of the following would be the MOST secure choice to implement for authenticating remote connections?

A. LDAP
B. 802.1x
C. RAS
D. RADIUS

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 48
An administrator wants to setup their network with only one public IP address. Which of the following would allow for this?

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

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 49
Which of the following allows an attacker to manipulate files by using the least significant bit(s) to secretly embed data?

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

Correct Answer: A
Section: Exam A
Explanation

Explanation/Reference:

QUESTION 50
Which of the following authentication methods would MOST likely prevent an attacker from being able to successfully deploy a replay attack?

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

Correct Answer: D
Section: Exam A
Explanation

Explanation/Reference:

Exam B

QUESTION 1
Which of the following may be an indication of a possible system compromise?

A. A port monitor utility shows that there are many connections to port 8 on the Internet facing web server.
B. A performance monitor indicates a recent and ongoing drop in speed, disk space or memory utilization from the baseline.
C. A protocol analyzer records a high number of UDP packets to a streaming media server on the Internet.
D. The certificate for one of the web servers has expired and transactions on that server begins to drop rapidly.

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is a best practice for coding applications in a secure manner?

A. Input validation.
B. Object oriented coding.
C. Rapid Application Development (RAD).
D. Cross-site scripting.

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 3
Which of the following logs would MOST likely indicate that there is an ongoing brute force attack against a server local administrator account?

A. Firewall
B. System
C. Performance
D. Access

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 4
Which of the following would be implemented to detect attacks on an individual system?

A. Firewall
B. Honeypot
C. NIPS

D. HIDS

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 5
Which of the following design elements could be set to only allow machines on the network if they are current with patches and antivirus definitions?

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

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 6
Which of the following behavior-based security appliances are used to prevent suspicious activity from entering the network?

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

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 7
Which of the following redundancy planning concepts is generally the MOST expensive?

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

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 8
A network administrator places a firewall between a file server and the public Internet and another firewall between the file server and the company internal servers. This is an example of which of the following design elements?

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

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 9
An administrator is required to keep certain workstations free of malware at all times, but those workstations need to be able to access any Internet site. Which of the following solutions would be the BEST choice?

A. Updated antivirus software.
B. Pop-up blockers.
C. Personal firewall.
D. Updated anti-spam software.

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 10
Which of the following encryption methods uses prime number factoring to obtain its strength?

A. Elliptic curve
B. RSA
C. AES
D. 3DES

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 11
A user reports that after searching the Internet for office supplies and visiting one of the search engine results websites, they began receiving unsolicited pop-ups on subsequent website visits. Which of the following is the MOST likely cause of the unsolicited pop-ups?

A. Virus
B. Trojan

C. Adware
D. Spam

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 12
Which of the following standards encodes in 64-bit sections, 56 of which are the encryption key?

A. SHA
B. AES
C. DES
D. Blowfish

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is a benefit of applying operating system service packs, patches, and hotfixes?

A. Protects systems from known vulnerabilities.
B. Minimizes the need to deploy honeypots.
C. Hardens systems against dictionary attacks.
D. Replaces default and guest accounts.

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 14
Backup tapes should be stored in which of the following?

A. Locked cabinet.
B. Waterproof safe within the data center.
C. Offsite location.
D. Fireproof safe near the backup server.

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 15
Which of the following describes what has occurred after a user has successfully gained access to a secure system?

A. Authentication
B. Authenticity
C. Identification
D. Confidentiality

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 16
A company has a problem with users inadvertently posting company information on the Internet. Which of the following is the BEST method for the company to address it?

A. Educate the users and perform awareness training.
B. Harden the password policies in case of future breaches.
C. Routinely audit all users browse history.
D. Implement HR policies with consequences.

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 17
Which of the following would be a benefit of testing a program of an unknown source on a virtual machine?

A. Virtual machines render it impossible for the code to escape.
B. Virtual machines allow for faster performance, so the speed of benchmark testing is increased.
C. Virtual machines come equipped with a firewall by default, thus preventing outside contamination.
D. Virtual machines can easily be restored to an earlier point if the code is malicious or causes instability.

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 18
Which of the following sends data packets to various IP ports on a host to determine the responsive ports?

A. OVAL
B. Network sniffer.
C. Protocol analyzer.
D. Network mappers.

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 19
A company wants to ensure that users only use their accounts between 8AM and 6PM Monday thru Friday. Which of the following access control methods would be MOST effective for this purpose?

A. Account expiration.
B. Logical tokens.
C. Time of day restrictions.
D. Group policies.

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 20
An administrator wishes to deploy an IPSec VPN connection between two routers across a WAN. The administrator wants to ensure that the VPN is encrypted in the most secure fashion possible. Which of the following BEST identifies the correct IPSec mode and the proper configuration?

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

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 21
Which of the following network protocols facilitates hiding internal addresses from the Internet?

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

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 22

Which of the following sends unsolicited messages to another user cell phone via Bluetooth?

A. Blue jacking
B. Smurfing
C. Data emanation
D. Bluesnarfing

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 23
Which of the following protocols are used to secure e-commerce transactions? (Select TWO).

A. TLS
B. IPSec
C. SSH
D. SSL
E. RTP

Correct Answer: AD
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 24
An instance where an IDS identifies legitimate traffic as malicious activity is called which of the following?

A. False positive
B. True negative
C. False negative
D. True positive

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 25
Multiple web servers are fed from a load balancer. Which of the following is this an example of?

A. RAID
B. Backup generator
C. Hot site
D. Redundant servers

Correct Answer: D
Section: Exam B

Explanation

Explanation/Reference:

QUESTION 26
After a period of high employee turnover, which of the following should be implemented?

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

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 27
Which of the following access control methods could the administrator implement because of constant hiring of new personnel?

A. Rule-based
B. Role-based
C. Discretionary
D. Decentralized

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 28
Which of the following access control methods could the administrator implement because of constant hiring of new personnel?

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

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 29
According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

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

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 30
Which of the following organizational documentation describes how tasks or job functions should be conducted?

A. Standards
B. Guideline
C. Policy
D. Procedures

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 31
A technician is deciding between implementing a HIDS on the database server or implementing a NIDS. Which of the following are reasons why a NIDS may be better to implement? (Select TWO).

A. Many HIDS require frequent patches and updates.
B. Many HIDS are not able to detect network attacks.
C. Many HIDS have a negative impact on system performance.
D. Many HIDS only offer a low level of detection granularity.
E. Many HIDS are not good at detecting attacks on database servers.

Correct Answer: BC
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 32
A user was trying to update an open file but when they tried to access the file they were denied. Which of the following would explain why the user could not access the file?

A. Audit only access.
B. Execute only access.
C. Rights are not set correctly.
D. Write only access.

Correct Answer: C

Section: Exam B
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is a security threat that hides itself within another piece of executable software?

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

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 34
Corporation has employed a third-party company to perform black-box penetration on their network. The corporation will provide:

A. Full access to the network, except user-created databases.
B. Unrestricted approved access, provided that every action is logged.
C. A test user account, but the company performs the network footprinting.
D. No information regarding their topology or technologies.

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 35
Which of the following allows a user to have a one-time password?

A. Biometrics
B. SSO
C. PIV
D. Tokens

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 36
Which of the following BEST describes the process of key escrow?

A. Maintains a copy of a user's public key for the sole purpose of recovering messages if it is lost.

B. Maintains a secured copy of a user's private key to recover the certificate revocation list.
C. Maintains a secured copy of a user's private key for the sole purpose of recovering the key if it is lost.
D. Maintains a secured copy of a user's public key in order to improve network performance.

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 37
A system administrator could have a user level account and an administrator account to prevent:

A. password sharing.
B. escalation of privileges.
C. implicit deny.
D. administrative account lockout.

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 38
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: Exam B
Explanation

Explanation/Reference:

QUESTION 39
Which of the following should be performed if a smartphone is lost to ensure no data can be retrieved from it?

A. Device encryption.
B. Remote wipe.
C. Screen lock.
D. GPS tracking.

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 40
A security administrator is implementing a solution that can integrate with an existing server and provide encryption capabilities. Which of the following would meet this requirement?

A. Mobile device encryption.
B. Full disk encryption.
C. TPM
D. HSM

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 41
Several classified mobile devices have been stolen. Which of the following would BEST reduce the data leakage threat?

A. Use GPS tracking to find the devices.
B. Use stronger encryption algorithms.
C. Immediately inform local law enforcement.
D. Remotely sanitize the devices.

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 42
Which of the following is used in conjunction with PEAP to provide mutual authentication between peers?

A. LEAP
B. MSCHAPv2
C. PPP
D. MSCHAPv1

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 43
Which of the following is an example of allowing a user to perform a self-service password reset?

A. Password length.
B. Password recovery.
C. Password complexity.
D. Password complexity.

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 44
A user is no longer able to transfer files to the FTP server. The security administrator has verified the ports are open on the network firewall. Which of the following should the security administrator check?

A. Anti-virus software
B. ACLs
C. Anti-spam software
D. NIDS

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 45
A user downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

A. Logic bomb
B. Worm
C. Trojan
D. Adware

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 46
NTLM is an improved and substantially backwards compatible replacement for which of the following?

A. 3DES
B. LANMAN
C. PGP
D. passwd

Correct Answer: B
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 47
A certificate that has been compromised should be published to which of the following?

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

Correct Answer: C
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 48
Actively monitoring data streams in search of malicious code or behavior is an example of:

A. load balancing.
B. an Internet proxy.
C. URL filtering.
D. content inspection.

Correct Answer: D
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 49
Which of the following tools provides the ability to determine if an application is transmitting a password in clear-text?

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

Correct Answer: A
Section: Exam B
Explanation

Explanation/Reference:

QUESTION 50
MAC filtering is a form of which of the following?

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

Correct Answer: B

Section: Exam B
Explanation

Explanation/Reference:

Exam C

QUESTION 1
A Human Resource manager is assigning access to users in their specific department performing the same job function. This is an example of:

A. role-based access control.
B. rule-based access control.
C. centralized access control.
D. mandatory access control.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 2
Which of the following methods of access, authentication, and authorization is the MOST secure by default?

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

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 3
In order to access the network, an employee must swipe their finger on a device. Which of the following describes this form of authentication?

A. Single-sign-on
B. Multifactor
C. Biometrics
D. Tokens

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 4
A new enterprise solution is currently being evaluated due to its potential to increase the company's profit margins. The security administrator has been asked to review its security implications. While evaluating the product, various vulnerability scans were performed. It was determined that the product is not a threat but has the potential to introduce additional vulnerabilities. Which of the following assessment types should the security administrator also take into consideration while evaluating this product?

A. Threat assessment
B. Vulnerability assessment
C. Code assessment
D. Risk assessment

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 5
In an 802.11n network, which of the following provides the MOST secure method of both encryption and authorization?

A. WEP with 802.1x
B. WPA Enterprise
C. WPA2-PSK
D. WPA with PKIP

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 6
Which of the following must a security administrator do when the private key of a web server has been compromised by an intruder?

A. Submit the public key to the CRL.
B. Use the recovery agent to revoke the key.
C. Submit the private key to the CRL.
D. Issue a new CA.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 7
DRPs should contain which of the following?

A. Hierarchical list of non-critical personnel
B. Hierarchical list of critical systems
C. Hierarchical access control lists
D. Identification of single points of failure

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 8
A security administrator with full administrative rights on the network is forced to change roles on a quarterly basis with another security administrator. Which of the following describes this form of access control?

A. Job rotation
B. Separation of duties
C. Mandatory vacation
D. Least privilege

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 9
An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

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

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 10
Which of the following wireless attacks uses a counterfeit base station with the same SSID name as a nearby intended wireless network?

A. War driving
B. Evil twin
C. Rogue access point
D. War chalking

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 11
A security administrator finished taking a forensic image of a computer's memory. Which of the following should the administrator do to ensure image integrity?

A. Run the image through AES128.
B. Run the image through a symmetric encryption algorithm.
C. Compress the image to a password protected archive.
D. Run the image through SHA256.

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 12
Which of the following is the BEST way to secure data for the purpose of retention?

A. Off-site backup
B. RAID 5 on-site backup
C. On-site clustering
D. Virtualization

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 13
Which of the following is specific to a buffer overflow attack?

A. Memory addressing
B. Directory traversal
C. Initial vector
D. Session cookies

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 14
Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

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

Correct Answer: BE
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 15
Which of the following protocols requires the use of a CA based authentication process?

A. FTPS implicit
B. FTPS explicit
C. MD5
D. PEAP-TLS

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 16
A thumbprint scanner is used to test which of the following aspects of human authentication?

A. Something a user did
B. Something a user has
C. Something a user is
D. Something a user knows

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 17
A targeted email attack sent to the company's Chief Executive Officer (CEO) is known as which of the following?

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

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 18
Which of the following facilitates computing for heavily utilized systems and networks?

A. Remote access
B. Provider cloud
C. VPN concentrator

D. Telephony

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 19
Which of the following should a security administrator implement to prevent users from disrupting network connectivity, if a user connects both ends of a network cable to different switch ports?

A. VLAN separation
B. Access control
C. Loop protection
D. DMZ

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 20
Which of the following security threats does shredding mitigate?

A. Shoulder surfing
B. Document retention
C. Tailgating
D. Dumpster diving

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 21
Which of the following uses TCP port 22 by default?

A. SSL, SCP, and TFTP
B. SSH, SCP, and SFTP
C. HTTPS, SFTP, and TFTP
D. TLS, TELNET, and SCP

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 22

Which of the following protocols should be blocked at the network perimeter to prevent host enumeration by sweep devices?

A. HTTPS
B. SSH
C. IPv4
D. ICMP

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 23
Which of the following would an administrator do to ensure that an application is secure and all unnecessary services are disabled?

A. Baselining
B. Application hardening
C. Secure application coding
D. Patch management

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 24
Which of the following elements of PKI are found in a browser's trusted root CA?

A. Private key
B. Symmetric key
C. Recovery key
D. Public key

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 25
Which of the following should the security administrator look at FIRST when implementing an AP to gain more coverage?

A. Encryption methods
B. Power levels
C. SSID
D. Radio frequency

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 26
Which of the following allows an attacker to identify vulnerabilities within a closed source software application?

A. Fuzzing
B. Compiling
C. Code reviews
D. Vulnerability scanning

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 27
Which of the following requires special handling and explicit policies for data retention and data distribution?

A. Personally identifiable information
B. Phishing attacks
C. Zero day exploits
D. Personal electronic devices

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 28
Which of the following is the primary purpose of using a digital signature? (Select TWO).

A. Encryption
B. Integrity
C. Confidentiality
D. Non-repudiation
E. Availability

Correct Answer: BD
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 29
A purpose of LDAP authentication services is:

A. to implement mandatory access controls.
B. a single point of user management.
C. to prevent multifactor authentication.
D. to issue one-time hashed passwords.

Correct Answer: B
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 30
Data can potentially be stolen from a disk encrypted, screen-lock protected, smartphone by which of the following?

A. Bluesnarfing
B. IV attack
C. Honeynet
D. SIM cloning

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 31
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses:

A. multiple keys for non-repudiation of bulk data.
B. different keys on both ends of the transport medium.
C. bulk encryption for data transmission over fiber.
D. the same key on each end of the transmission medium.

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 32
An administrator is updating firmware on routers throughout the company. Where should the administrator document this work?

A. Event Viewer
B. Router's System Log
C. Change Management System
D. Compliance Review System

Correct Answer: C
Section: Exam C

Explanation

Explanation/Reference:

QUESTION 33
Which of the following is the BEST way to mitigate data loss if a portable device is compromised?

A. Full disk encryption.
B. Common access card.
C. Strong password complexity.
D. Biometric authentication.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 34
A security administrator is asked to email an employee their password. Which of the following account policies MUST be set to ensure the employee changes their password promptly?

A. Password expiration
B. Account lockout
C. Password recovery
D. Account enablement

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 35
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: Exam C
Explanation

Explanation/Reference:

QUESTION 36
Centrally authenticating multiple systems and applications against a federated user database is an example of:

A. smart card.

B. common access card.
C. single sign-on.
D. access control list.

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 37
In which of the following locations would a forensic analyst look to find a hooked process?

A. BIOS
B. Slack space
C. RAM
D. Rootkit

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is an example of requiring users to have a password of 16 characters or more?

A. Password recovery requirements
B. Password complexity requirements
C. Password expiration requirements
D. Password length requirements

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 39
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: Exam C
Explanation

Explanation/Reference:

QUESTION 40
While browsing the Internet, an administrator notices their browser behaves erratically, appears to download something, and then crashes. Upon restarting the PC, the administrator notices performance is extremely slow and there are hundreds of outbound connections to various websites. Which of the following BEST describes what has occurred?

A. The PC has become part of a botnet.
B. The PC has become infected with spyware.
C. The PC has become a spam host.
D. The PC has become infected with adware.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 41
A web application has been found to be vulnerable to a SQL injection attack. Which of the following BEST describes the required remediation action?

A. Change the server's SSL key and add the previous key to the CRL.
B. Install a host-based firewall.
C. Install missing security updates for the operating system.
D. Add input validation to forms.

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 42
Risk can be managed in the following ways EXCEPT:

A. mitigation.
B. acceptance.
C. elimination.
D. transference.

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 43
A user reports that their 802.11n capable interface connects and disconnects frequently to an access point that was recently installed. The user has a Bluetooth enabled laptop. A company in the next building had their wireless network breached last month. Which of the following is MOST likely causing the disconnections?

A. An attacker inside the company is performing a bluejacking attack on the user's laptop.

B. Another user's Bluetooth device is causing interference with the Bluetooth on the laptop.
C. The new access point was mis-configured and is interfering with another nearby access point.
D. The attacker that breached the nearby company is in the parking lot implementing a war driving attack.

Correct Answer: C
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 44
Which of the following BEST describes an intrusion prevention system?

A. A system that stops an attack in progress.
B. A system that allows an attack to be identified.
C. A system that logs the attack for later analysis.
D. A system that serves as a honeypot.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 45
Which of the following concepts ensures that the data is only viewable to authorized users?

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

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 46
A security administrator has discovered through a password auditing software that most passwords can be discovered by cracking the first seven characters and then cracking the second part of the password. Which of the following is in use by the company?

A. LANMAN
B. MD5
C. WEP
D. 3DES

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is MOST likely to result in data loss?

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

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 48
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: Exam C
Explanation

Explanation/Reference:

QUESTION 49
Which of the following BEST describes the proper method and reason to implement port security?

A. Apply a security control which ties specific ports to end-device MAC addresses and prevents additional devices from being connected to the network.
B. Apply a security control which ties specific networks to end-device IP addresses and prevents new devices from being connected to the network.
C. Apply a security control which ties specific ports to end-device MAC addresses and prevents all devices from being connected to the network.
D. Apply a security control which ties specific ports to end-device IP addresses and prevents mobile devices from being connected to the network.

Correct Answer: A
Section: Exam C
Explanation

Explanation/Reference:

QUESTION 50
Which of the following methods BEST describes the use of hiding data within other files?

A. Digital signatures.
B. PKI
C. Transport encryption
D. Steganography

Correct Answer: D
Section: Exam C
Explanation

Explanation/Reference:

Exam D

QUESTION 1
Which of the following is a reason to perform a penetration test?

A. To passively test security controls within the enterprise.
B. To provide training to white hat attackers.
C. To identify all vulnerabilities and weaknesses within the enterprise.
D. To determine the impact of a threat against the enterprise.

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 2
If a user wishes to receive a file encrypted with PGP, the user must FIRST supply the:

A. public key.
B. recovery agent.
C. key escrow account.
D. private key.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 3
Which of the following will educate employees about malicious attempts from an attacker to obtain bank account information?

A. Password complexity requirements
B. Phishing techniques
C. Handling PII
D. Tailgating techniques

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is the BEST choice for encryption on a wireless network?

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

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 5
Which of the following should be enabled to ensure only certain wireless clients can access the network?

A. DHCP
B. SSID broadcast
C. MAC filtering
D. AP isolation

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 6
The security administrator is getting reports from users that they are accessing certain websites and are unable to download anything off of those sites. The security administrator is also receiving several alarms from the IDS about suspicious traffic on the network. Which of the following is the MOST likely cause?

A. NIPS is blocking activities from those specific websites.
B. NIDS is blocking activities from those specific websites.
C. The firewall is blocking web activity.
D. The router is denying all traffic from those sites.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 7
Which of the following describes a passive attempt to identify weaknesses?

A. Vulnerability scanning.

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

B. Zero day attack.
C. Port scanning.
D. Penetration testing.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 8
Which of the following PKI implementation element is responsible for verifying the authenticity of certificate contents?

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

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 9
Which of the following BEST describes the function of TPM?

A. High speed secure removable storage device.
B. Third party certificate trust authority.
C. Hardware chip that stores encryption keys.
D. A trusted OS model.

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 10
Which of the following is used when performing a quantitative risk analysis?

A. Focus groups
B. Asset value
C. Surveys
D. Best practice

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 11
Which of the following environmental controls would BEST be used to regulate cooling within a datacenter?

A. Fire suppression
B. Video monitoring.
C. EMI shielding.
D. Hot and cold aisles.

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 12
A security administrator wants to prevent users in sales from accessing their servers after 6:00 p.m., and prevent them from accessing accounting's network at all times. Which of the following should the administrator implement to accomplish these goals? (Select TWO).

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

Correct Answer: BC
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 13
Which of the following cloud computing concepts is BEST described as providing an easy-to- configure OS and on-demand computing for customers?

A. Platform as a Service
B. Software as a Service
C. Infrastructure as a Service
D. Trusted OS as Service

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 14
Which of the following devices BEST allows a security administrator to identify malicious activity after it has occurred?

A. Spam filter
B. IDS
C. Firewall
D. Malware inspection

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 15
Which of the following penetration testing types is performed by security professionals with limited inside knowledge of the network?

A. Passive vulnerability scan.
B. Gray box.
C. White box.
D. Black box.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 16
Public keys are used for which of the following?

A. Decrypting wireless messages.
B. Decrypting the hash of an electronic signature.
C. Bulk encryption of IP based email traffic.
D. Encrypting web browser traffic.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 17
Which of the following is a technical control?

A. System security categorization requirement.
B. Baseline configuration development.
C. Contingency planning.
D. Least privilege implementation.

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 18
Which of the following is an example of verifying new software changes on a test system?

A. User access control.
B. Patch management.
C. Intrusion prevention.
D. Application hardening.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is true about hardware encryption? (Select TWO).

A. It must use elliptical curve encryption.
B. It requires a HSM file system.
C. It only works when data is not highly fragmented.
D. It is faster than software encryption.
E. It is available on computers using TPM.

Correct Answer: DE
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 20
During the analysis of malicious code, a security analyst discovers JavaScript being used to send random data to another service on the same system. This is MOST likely an example of which of the following?

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

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is MOST likely to be the last rule contained on any firewall?

A. IP allow any any
B. Implicit deny.
C. Separation of duties.
D. Time of day restrictions.

Correct Answer: B
Section: Exam D

Explanation

Explanation/Reference:

QUESTION 22
Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

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

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 23
Isolation mode on an AP provides which of the following functionality types?

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

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 24
A penetration test shows that almost all database servers were able to be compromised through a default database user account with the default password. Which of the following is MOST likely missing from the operational procedures?

A. Application hardening.
B. OS hardening.
C. Application patch management.
D. SQL injection.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 25
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: Exam D
Explanation

Explanation/Reference:

QUESTION 26
Which of the following devices would be installed on a single computer to prevent intrusion?

A. Host intrusion detection.
B. Network firewall.
C. Host-based firewall.
D. VPN concentrator.

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 27
Which of the following would allow traffic to be redirected through a malicious machine by sending false hardware address updates to a switch?

A. ARP poisoning.
B. MAC spoofing.
C. pWWN spoofing.
D. DNS poisoning.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 28
Which of the following would be the BEST action to perform when conducting a corporate vulnerability assessment?

A. Document scan results for the change control board.
B. Organize data based on severity and asset value.
C. Examine the vulnerability data using a network analyzer.
D. Update antivirus signatures and apply patches.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 29
Which of the following access control technologies provides a rolling password for one-time use?

A. RSA tokens.
B. ACL
C. Multifactor authentication.
D. PIV card.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 30
Which of the following web application security weaknesses can be mitigated by preventing the use of HTML tags?

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

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 31
Performing routine security audits is a form of which of the following controls?

A. Preventive
B. Detective
C. Protective
D. Proactive

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 32
The security administrator implemented privacy screens, password protected screen savers, and hired a secure shredding and disposal service. Which of the following attacks is the security administrator trying to mitigate? (Select TWO).

A. Whaling

B. Dumpster diving
C. Shoulder surfing
D. Tailgating
E. Impersonation

Correct Answer: BC
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 33
Due to sensitive data concerns, a security administrator has enacted a policy preventing the use of flash drives. Additionally, which of the following can the administrator implement to reduce the risk of data leakage?

A. Enact a policy that all work files are to be password protected.
B. Enact a policy banning users from bringing in personal music devices.
C. Provide users with unencrypted storage devices that remain on-site.
D. Disallow users from saving data to any network share.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 34
Which of the following file transfer protocols is an extension of SSH?

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

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 35
Which of the following uses tickets to identify users to the network?

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

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 36
Which of the following security practices should occur initially in software development?

A. Secure code review.
B. Patch management.
C. Fuzzing.
D. Penetration tests.

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 37
Which of the following should be used to help prevent device theft of unused assets?

A. HSM device.
B. Locking cabinet.
C. Device encryption.
D. GPS tracking.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is seen as non-secure based on its ability to only store seven uppercase characters of data making it susceptible to brute force attacks?

A. PAP
B. NTLMv2
C. LANMAN
D. CHAP

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 39
Which of the following MUST a programmer implement to prevent cross-site scripting?

A. Validate input to remove shell scripts.
B. Validate input to remove hypertext.
C. Validate input to remove batch files.

D. Validate input to remove Java bit code.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 40
When examining HTTP server logs the security administrator notices that the company's online store crashes after a particular search string is executed by a single external user. Which of the following BEST describes this type of attack?

A. Spim
B. DDoS
C. Spoofing
D. DoS

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 41
A security administrator needs to implement a site-to-site VPN tunnel between the main office and a remote branch. Which of the following protocols should be used for the tunnel?

A. RTP
B. SNMP
C. IPSec
D. 802.1x

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 42
A small company needs to invest in a new expensive database. The company's budget does not include the purchase of additional servers or personnel. Which of the following solutions would allow the small company to save money on hiring additional personnel and minimize the footprint in their current datacenter?

A. Allow users to telecommute.
B. Setup a load balancer.
C. Infrastructure as a Service.
D. Software as a Service.

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 43
Which of the following devices provides storage for RSA or asymmetric keys and may assist in user authentication? (Select TWO).

A. Trusted platform module.
B. Hardware security module.
C. Facial recognition scanner.
D. Full disk encryption.
E. Encrypted USB.

Correct Answer: AB
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 44
An administrator in a small office environment has implemented an IDS on the network perimeter to detect malicious traffic patterns. The administrator still has a concern about traffic inside the network originating between client workstations. Which of the following could be implemented?

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

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 45
A technician is testing the security of a new database application with a website front-end. The technician notices that when certain characters are input into the application it will crash the server. Which of the following does the technician need to do?

A. Utilize SSL on the website.
B. Implement an ACL.
C. Lock-down the database.
D. Input validation.

Correct Answer: D
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 46
Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned

that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Install anti-virus software on the USB drives.
C. Disable USB within the workstation BIOS.
D. Apply the concept of least privilege to USB devices.
E. Run spyware detection against all workstations.

Correct Answer: AC
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 47
Which of the following is the MOST secure alternative for administrative access to a router?

A. SSH
B. Telnet
C. rlogin
D. HTTP

Correct Answer: A
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 48
When should a technician perform penetration testing?

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

Correct Answer: C
Section: Exam D
Explanation

Explanation/Reference:

QUESTION 49
Why would a technician use a password cracker?

A. To look for weak passwords on the network.
B. To change a user passwords when they leave the company.
C. To enforce password complexity requirements.
D. To change user passwords if they have forgotten them.

Correct Answer: A

Section: Exam D
Explanation

Explanation/Reference:

QUESTION 50
When is the BEST time to update antivirus definitions?

A. At least once a week as part of system maintenance.
B. As the definitions become available from the vendor.
C. When a new virus is discovered on the system.
D. When an attack occurs on the network.

Correct Answer: B
Section: Exam D
Explanation

Explanation/Reference:

Exam E

QUESTION 1
Which of the following BEST describes the term war driving?

A. Driving from point to point with a laptop and an antenna to find unsecured wireless access points.
B. Driving from point to point with a wireless scanner to read other user emails through the access point.
C. Driving from point to point with a wireless network card and hacking into unsecured wireless access points.
D. Driving from point to point with a wireless scanner to use unsecured access points.

Correct Answer: A
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 2
Which of following can BEST be used to determine the topology of a network and discover unknown devices?

A. Vulnerability scanner.
B. NIPS
C. Protocol analyzer
D. Network mapper

Correct Answer: D
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 3
After issuance a technician becomes aware that some keys were issued to individuals who are not authorized to use them. Which of the following should the technician use to correct this problem?

A. Recovery agent.
B. Certificate revocation list.
C. Key escrow.
D. Public key recovery.

Correct Answer: B
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 4
Which of the following should a technician recommend to prevent physical access to individual office areas? (Select TWO).

A. Video surveillance.
B. Blockade.
C. Key card readers.

D. Mantrap.
E. Perimeter fence.

Correct Answer: CD
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 5
Which of the following tools will allow the technician to find all open ports on the network?

A. Performance monitor.
B. Protocol analyzer.
C. Router ACL.
D. Network scanner.

Correct Answer: D
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 6
Which of the following is an exploit against a device where only the hardware model and manufacturer are known?

A. Replay attack.
B. Denial of service (DoS).
C. Privilege escalation.
D. Default password.

Correct Answer: D
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 7
Which of the following methods is used to perform denial of service (DoS) attacks?

A. Privilege escalation
B. Botnet
C. Adware
D. Spyware

Correct Answer: B
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 8
User A is a member of the payroll security group. Each member of the group should have read/write permissions to a share. User A was trying to update a file but when the user tried to access the file the user was denied. Which of the following would explain why User A could not access the file?

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

Correct Answer: B
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 9
Which of the following is an example of security personnel that administer access control functions, but do not administer audit functions?

A. Access enforcement.
B. Separation of duties.
C. Least privilege.
D. Account management.

Correct Answer: B
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 10
A technician needs to detect staff members that are connecting to an unauthorized website. Which of the following could be used?

A. Protocol analyzer.
B. Bluesnarfing.
C. Host routing table.
D. HIDS

Correct Answer: A
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 11
Which of the following algorithms is the LEAST secure?

A. NTLM
B. MD5

C. LANMAN
D. SHA-1

Correct Answer: C
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 12
Which of the following security policies is BEST to use when trying to mitigate the risks involved with allowing a user to access company email via their cell phone?

A. The cell phone should require a password after a set period of inactivity.
B. The cell phone should only be used for company related emails.
C. The cell phone data should be encrypted according to NIST standards.
D. The cell phone should have data connection abilities disabled.

Correct Answer: A
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 13
Which of the following redundancy solutions contains hardware systems similar to the affected organization, but does not provide live data?

A. Hot site.
B. Uninterruptible Power Supply (UPS).
C. Warm site.
D. Cold site.

Correct Answer: C
Section: Exam E
Explanation

Explanation/Reference:

QUESTION 14
An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

A. Spyware
B. Trojan
C. Privilege escalation
D. DoS

Correct Answer: D
Section: Exam E
Explanation

Explanation/Reference:

http://www.gratisexam.com/