SY0-301.07102012

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

http://www.gratisexam.com/

Exam Name: CompTIA Security+ 2011 Exam
Exam Type: CampTIA Exam Code: SY0-301
Certification Security+ Total Questions: 737

A Network Security
B Compliance and Operational Security
C Threats and Vulnerabilities
D Application, Data and Host Security
E Access Control and Identity Management
F Cryptography
G Mixed Questions

Powered by.....

Good Study Websites:

http://www.professormesser.com/free-comptia-security-training/security-plus-videos/
http://www.proprofs.com/mwiki/index.php?title=Comptia_Security%2B_Certification_Exam
http://www.techexams.net/cotechnotes.shtml

Exam A

QUESTION 1
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: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following network devices would MOST likely be used to detect but not react to suspicious behavior on the network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which of the following can a security administrator implement to help identify smurf attacks?

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

A. Load balancer
B. Spam filters
C. NIDS
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following wireless security controls can be easily and quickly circumvented using only a network sniffer? (Select TWO).

A. MAC filtering
B. Disabled SSID broadcast
C. WPA2-Enterprise
D. EAP-TLS
E. WEP with 802.1x

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following functions is MOST likely performed by a web security gateway?

A. Protocol analyzer

B. Content filtering
C. Spam filtering
D. Flood guard

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following devices is often used to cache and filter content?

A. Proxies
B. Firewall
C. VPN
D. Load balancer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
In order to provide flexible working conditions, a company has decided to allow some employees remote access into corporate headquarters. Which of the following security technologies could be used to provide remote access? (Select TWO).

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following devices is used to optimize and distribute data workloads across multiple computers or networks?

A. Load balancer
B. URL filter
C. VPN concentrator
D. Protocol analyzer

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 11
An IT administrator wants to provide 250 staff with secure remote access to the corporate network. Which of the following BEST achieves this requirement?

A. Software based firewall
B. Mandatory Access Control (MAC)
C. VPN concentrator
D. Web security gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following should be installed to prevent employees from receiving unsolicited emails?

A. Pop-up blockers
B. Virus definitions
C. Spyware definitions
D. Spam filters

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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: (none)
Explanation

Explanation/Reference:

QUESTION 14
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: (none)
Explanation

Explanation/Reference:

QUESTION 15
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: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which of the following would need to be configured correctly to allow remote access to the network?

A. ACLs
B. Kerberos
C. Tokens
D. Biometrics

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
By default, which of the following stops network traffic when the traffic is not identified in the firewall rule set?

A. Access control lists
B. Explicit allow
C. Explicit deny
D. Implicit deny

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Based on logs from file servers, remote access systems, and IDS, a malicious insider was stealing data using a personal laptop while connected by VPN. The affected company wants access to the laptop to determine loss, but the insider's lawyer insists the laptop cannot be identified. Which of the following would BEST be used to identify the specific computer used by the insider?

A. IP address
B. User profiles
C. MAC address
D. Computer name

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Applying detailed instructions to manage the flow of network traffic at the edge of the network, including allowing or denying traffic based on port, protocol, address, or direction is an implementation of which of the following?

A. Virtualization
B. Port security
C. IPSec
D. Firewall rules

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following is the default rule found in a corporate firewall's access control list?

A. Anti-spoofing
B. Permit all
C. Multicast list
D. Deny all

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following is BEST used to prevent ARP poisoning attacks across a network?

A. VLAN segregation
B. IPSec
C. IP filters
D. Log analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is MOST likely to be the last rule contained on any firewall?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 a Service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
MAC filtering is a form of which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Reviewing an access control list on a firewall reveals a Drop All statement at the end of the rules. Which of the following describes this form of access control?

A. Discretionary
B. Time of day restrictions
C. Implicit deny
D. Mandatory

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
An administrator is taking an image of a server and converting it to a virtual instance. Which of the following BEST describes the information security requirements of a virtualized server?

A. Virtual servers require OS hardening but not patching or antivirus.
B. Virtual servers have the same information security requirements as physical servers.
C. Virtual servers inherit information security controls from the hypervisor.
D. Virtual servers only require data security controls and do not require licenses.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

Web mail is classified under which of the following cloud-based technologies?

A. Demand Computing
B. Infrastructure as a Service (IaaS)
C. Software as a Service (SaaS)
D. Platform as a Service (PaaS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A security engineer is troubleshooting a server in the DMZ, which cannot be reached from the Internet or the internal network. All other servers on the DMZ are able to communicate with this server. Which of the following is the MOST likely cause?

A. The server is configured to reject ICMP packets.
B. The server is on the external zone and it is configured for DNS only.
C. The server is missing the default gateway.
D. The server is on the internal zone and it is configured for DHCP only.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following may cause a user, connected to a NAC-enabled network, to not be prompted for credentials?

A. The user's PC is missing the authentication agent.
B. The user's PC is not fully patched.
C. The user's PC is not at the latest service pack.
D. The user's PC has out-of-date antivirus software.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following would be implemented to allow access to services while segmenting access to the internal network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A security administrator needs to separate two departments. Which of the following would the administrator implement to perform this?

A. Cloud computing
B. VLAN
C. Load balancer
D. MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is a security control that is lost when using cloud computing?

A. Logical control of the data
B. Access to the application's administrative settings
C. Administrative access to the data
D. Physical control of the data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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: (none)
Explanation

Explanation/Reference:

QUESTION 35

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: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which of the following allows a security administrator to set device traps?

A. SNMP
B. TLS
C. ICMP
D. SSH

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following protocols would be the MOST secure method to transfer files from a host machine?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 39
Which of the following port numbers is used for SCP, by default?

A. 22
B. 69
C. 80
D. 443

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following is the MOST secure method of utilizing FTP?

A. FTP active
B. FTP passive
C. SCP
D. FTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following protocols can be implemented to monitor network devices?

A. IPSec
B. FTPS
C. SFTP
D. SNMP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following protocols would an administrator MOST likely use to monitor the parameters of network devices?

A. SNMP

B. NetBIOS
C. ICMP
D. SMTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A remote office is reporting they are unable to access any of the network resources from the main office. The security administrator realizes the error and corrects it. The administrator then tries to ping the router at the remote office and receives no reply; however, the technician is able to telnet to that router. Which of the following is the MOST likely cause of the security administrator being unable to ping the router?

A. The remote switch is turned off.
B. The remote router has ICMP blocked.
C. The remote router has IPSec blocked.
D. The main office's router has ICMP blocked.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A network administrator is implementing a network addressing scheme that uses a long string of both numbers and alphanumeric characters to create addressing options and avoid duplicates. Which of the following describes a protocol built for this purpose?

A. IPv6
B. ICMP
C. IGMP
D. IPv4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following file transfer protocols is an extension of SSH?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following secure protocols is MOST commonly used to remotely administer Unix/Linux systems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
The security administrator notices a number of TCP connections from the development department to the test network segregation. Large volumes of data are being transmitted between the two networks only on port 22. Which of the following is MOST likely occurring?

A. The development team is transferring data to test systems using FTP and TFTP.
B. The development team is transferring data to test systems using SCP and TELNET.
C. The development team is transferring data to test systems using SFTP and SCP.
D. The development team is transferring data to test systems using SSL and SFTP.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An administrator who wishes to block all database ports at the firewall should include which of the following ports in the block list?

A. 445
B. 1433
C. 1501
D. 3389

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
If a security administrator wants to TELNET into a router to make configuration changes, which of the following ports would need to be open by default?

A. 23
B. 135
C. 161
D. 3389

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following ports would a security administrator block if the administrator wanted to stop users from accessing outside SMTP services?

A. 21
B. 25
C. 110
D. 143

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
A network consists of various remote sites that connect back to two main locations. The security administrator needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site.
B. Block port 23 on the network firewall.
C. Block port 25 on the L2 switch at each remote site.
D. Block port 25 on the network firewall.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Which of the following are the default ports for HTTP and HTTPS protocols? (Select TWO).

A. 21
B. 80
C. 135
D. 443
E. 445

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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: (none)
Explanation

Explanation/Reference:

QUESTION 55
Isolation mode on an AP provides which of the following functionality types?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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: (none)
Explanation

Explanation/Reference:

QUESTION 57
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: (none)
Explanation

Explanation/Reference:

QUESTION 58
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: (none)
Explanation

Explanation/Reference:

QUESTION 59
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: (none)
Explanation

Explanation/Reference:

QUESTION 60
When configuring multiple computers for RDP on the same wireless router, it may be necessary to do which of the following?

A. Forward to different RDP listening ports.
B. Turn off port forwarding for each computer.
C. Enable DMZ for each computer.
D. Enable AP isolation on the router.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A technician needs to limit the wireless signal from reaching outside of a building. Which of the following actions should the technician take?

A. Disable the SSID broadcast on the WAP
B. Place the WAP antenna on the exterior wall of the building
C. Decrease the power levels on the WAP
D. Enable MAC filtering in the WAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following will provide the HIGHEST level of wireless network security?

A. WPA2
B. SSH
C. SSID
D. WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Topic 2, Compliance and Operational Security

QUESTION 63
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: (none)
Explanation

Explanation/Reference:

QUESTION 64
Risk can be managed in the following ways EXCEPT:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A company that purchases insurance to reduce risk is an example of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is a best practice to identify fraud from an employee in a sensitive position?

A. Acceptable usage policy
B. Separation of duties
C. False positives
D. Mandatory vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
A security administrator with full administrative rights on the network is forced to temporarily take time off of their duties. Which of the following describes this form of access control?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
Instead of giving a security administrator full administrative rights on the network, the administrator is given rights only to review logs and update security related network devices. Additional rights are handed out to network administrators for the areas that fall within their job description. Which of the following describes this form of access control?

A. Mandatory vacation
B. Least privilege
C. Discretionary
D. Job rotation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security administrator wants to determine what data is allowed to be collected from users of the corporate Internet-facing web application. Which of the following should be referenced?

A. Privacy policy
B. Human Resources policy
C. Appropriate use policy
D. Security policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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: (none)
Explanation

Explanation/Reference:

QUESTION 71
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: (none)
Explanation

Explanation/Reference:

QUESTION 72
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: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following is MOST commonly a part of routine system audits?

A. Job rotation
B. Business impact analysis
C. User rights and permissions reviews
D. Penetration testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is a method to prevent ad-hoc configuration mistakes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which of the following should be reviewed periodically to ensure a server maintains the correct security configuration?

A. NIDS configuration
B. Firewall logs
C. User rights
D. Incident management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following BEST explains the security benefit of a standardized server image?

A. All current security updates for the operating system will have already been applied.
B. Mandated security configurations have been made to the operating system.

C. Anti-virus software will be installed and current.
D. Operating system license use is easier to track.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Which of the following describes when forensic hashing should occur on a drive?

A. After the imaging process and before the forensic image is captured
B. Before the imaging process and then after the forensic image is created
C. After the imaging process and after the forensic image is captured
D. Before and after the imaging process and then hash the forensic image

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following assists in identifying if a system was properly handled during transport?

A. Take a device system image
B. Review network traffic and logs
C. Track man hours and incident expense
D. Chain of custody

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following describes the purpose of chain of custody as applied to forensic image retention?

A. To provide proof the evidence has not been tampered with or modified
B. To provide verification that the forensic examiner is qualified
C. To provide documentation as to who has handled the evidence
D. To provide a baseline reference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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:

QUESTION 82
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: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following is a reason to perform user awareness and training?

A. To enforce physical security requirements by staff
B. To minimize the organizational risk posed by users
C. To comply with law and vendor software best practices
D. To identify the staff's personally owned electronic devices

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie
C. Pet's name
D. Birthday
E. Full name

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
On-going annual awareness security training should be coupled with:

A. Succession planning.
B. Implementation of security controls.
C. User rights and permissions review.
D. Signing of a user agreement.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which of the following risks may result from improper use of social networking and P2P software?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is the MAIN reason to require data labeling?

A. To ensure that staff understands what data they are handling and processing
B. To ensure that new viruses do not transfer to removable media
C. To ensure that all media sanitization requirements are met
D. To ensure that phishing attacks are identified and labeled properly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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: (none)
Explanation

Explanation/Reference:

QUESTION 89
Recovery Point Objectives and Recovery Time Objectives directly relate to which of the following BCP concepts?

A. Succession planning
B. Remove single points of failure
C. Risk management
D. Business impact analysisx

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security firm has been engaged to assess a software application. A production-like test environment, login details, production documentation and source code have been provided. Which of the following types of testing is being described?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following environmental controls would BEST be used to regulate cooling within a datacenter?

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following environmental variables reduces the potential for static discharges?

A. EMI
B. Temperature
C. UPS
D. Humidity

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following should be considered when trying to prevent somebody from capturing network traffic?

A. Video monitoring
B. Hot aisles
C. HVAC controls
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
With which of the following is RAID MOST concerned?

A. Integrity
B. Confidentiality
C. Availability
D. Base lining

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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:

QUESTION 96
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: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security administrator is tasked with ensuring that all servers are highly available and that hard drive failure will not affect an individual server. Which of the following configurations will allow for high availability? (Select TWO).

A. Hardware RAID 5
B. Load sharing
C. Server clustering
D. Software RAID 1
E. Load balancing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A security administrator is in charge of a datacenter, a hot site and a cold site. Due to a recent disaster, the administrator needs to ensure that their cold site is ready to go in case of a disaster. Which of the following does the administrator need to ensure is in place for a cold site?

A. Location with all required equipment loaded with all current patches and updates

B. Location with duplicate systems found in the datacenter
C. Location near the datacenter that meets power requirements
D. Location that meets power and connectivity requirements

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A critical system in the datacenter is not connected to a UPS. The security administrator has coordinated an authorized service interruption to resolve this issue. This is an example of which of the following?

A. Fault tolerance
B. Continuity of operations
C. Succession planning
D. Data handling error

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In order to ensure high availability of all critical servers, backups of the main datacenter are done in the middle of the night and then the backup tapes are taken to an offsite location. Which of the following would ensure the minimal amount of downtime in the case of a disaster?

A. Having the offsite location of tapes also be the standby server
B. Having the offsite location of tapes also be the warm site
C. Having the offsite location of tapes also be the cold site
D. Having the offsite location of tapes also be the hot site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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: (none)
Explanation

Explanation/Reference:

QUESTION 102
A security administrator working for a health insurance company needs to protect customer data by installing an HVAC system and a mantrap in the datacenter. Which of the following are being addressed? (Select TWO).

A. Integrity
B. Recovery
C. Clustering
D. Confidentiality
E. Availability

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A bulk update process fails and writes incorrect data throughout the database. Which of the following concepts describes what has been compromised?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 3, Threats and Vulnerabilities

QUESTION 104
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 EST describes this type of malware?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
While browsing the Internet, an administrator notices their browser behaves erratically, appears downloading

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: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following malware types is an antivirus scanner MOST unlikely to discover? (Select TWO).

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is the primary difference between a virus and a worm?

A. A worm is undetectable
B. A virus is typically larger
C. A virus is easily removed
D. A worm is self-replicating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Logs from an IDS show that a computer has been compromised with a botnet and is actively communicating with a command and control server. If the computer is powered off, which of the following data types will be unavailable for later investigation?

A. Swap files, system processes, and master boot record
B. Memory, temporary file system, and archival storage
C. System disk, email, and log files

D. Memory, network processes, and system processes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Upon investigation, an administrator finds a suspicious system-level kernel module which modifies file system operations. This is an example of which of the following?

A. Trojan
B. Virus
C. Logic bomb
D. Rootkit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following is the MOST likely cause of a single computer communicating with an unknown IRC server and scanning other systems on the network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following malware types is MOST commonly installed through the use of thumb rives to compromise systems and provide unauthorized access?

A. Trojans
B. Bonnets
C. Adware
D. Logic bomb

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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: (none)
Explanation

Explanation/Reference:

QUESTION 113
When examining HTTP server logs the security administrator notices that the company's online tore 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: (none)
Explanation

Explanation/Reference:

QUESTION 114
Which of the following would allow traffic to be redirected through a malicious machine by ending False hardware address updates to a switch?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which of the following threats corresponds with an attacker targeting specific employees of a company?

A. Spear phishing
B. Phishing
C. Pharming

D. Man-in-the-middle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A user receives an automated call which appears to be from their bank. The automated recording provides details about the bank's privacy policy, security policy and requests that the user clearly Tate their name, birthday and enter the banking details to validate the user's identity. Which of the following BEST describes this type of attack?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which of the following is a technique designed to obtain information from a specific person?

A. Smurf attack
B. Spear phishing
C. DNS poisoning
D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following is another name for a malicious attacker?

A. Black hat
B. White hat
C. Penetration tester
D. Fuzzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Which of the following logical controls does a flood guard protect against?

A. Spanning tree
B. Xmas attacks
C. Botnet attack
D. SYN attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following attacks is BEST described as the interruption of network traffic accompanied by the insertion of malicious code?

A. Spoofing
B. Man-in-the-middle
C. Spear phishing
D. DoS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A targeted email attack sent to the company's Chief Executive Officer (CEO) is known as which f he following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following security threats does shredding mitigate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following attacks would password masking help mitigate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following is an example of allowing another user physical access to a secured area without validation of their credentials?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following wireless attacks uses a counterfeit base station with the same SSID name s a nearby intended wireless network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Data can potentially be stolen from a disk encrypted, screen-lock protected, smart phone by which f the following?

A. Bluesnarfing
B. IV attack
C. Honey net
D. SIM cloning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Which of the following is an unauthorized wireless router that allows access to a secure network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A security administrator performs several war driving routes each month and recently has noticed certain area with a large number of unauthorized devices. Which of the following attack types is OST likely occurring?

A. Interference
B. Rogue access points
C. IV attack
D. Blue jacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Proper wireless antenna placement and radio power setting reduces the success of which of the following reconnaissance methods?

A. Rogue APs
B. War driving
C. Packet analysis
D. RF interference

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A rogue access point with the same SSID as the production wireless network is found. Which of he following BEST describes this attack?

A. Evil twin
B. Vishing
C. War driving
D. Bluesnarfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A programmer allocates 16 bytes for a string variable, but does not adequately ensure that more than 16 bytes cannot be copied into the variable. This program may be vulnerable to which of the following attacks?

A. Buffer overflow
B. Cross-site scripting
C. Session hijacking
D. Directory traversal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following web application security weaknesses can be mitigated by preventing the se of HTML tags?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
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: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following attacks is manifested as an embedded HTML image object or JavaScript mage 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:

QUESTION 138
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: (none)
Explanation

Explanation/Reference:

QUESTION 139
An application log shows that the text "test; rm -rf /etc/passed" was entered into an HTML form. Which of the following describes the type of attack that was attempted?

A. Session hijacking
B. Command injection
C. Buffer overflow
D. SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following is MOST relevant to a buffer overflow attack?

A. Sequence numbers
B. Set flags
C. IV length
D. NOOP instructions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
The detection of a NOOP sled is an indication of which of the following attacks?

A. SQL injection
B. Buffer overflow
C. Cross-site scripting
D. Directory transversal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
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: (none)
Explanation

Explanation/Reference:

QUESTION 143
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: (none)
Explanation

Explanation/Reference:

QUESTION 144
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 honey pot.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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:

QUESTION 146
Which of the following can prevent an unauthorized employee from entering a datacenter? Select TWO).

A. Failsafe
B. Video surveillance
C. Bollards
D. Security guard
E. Proximity reader

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Two systems are being designed. System A has a high availability requirement. System B has a high security requirement with less emphasis on system uptime. Which of the following configurations BEST fits the need for each system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Several staff members working in a datacenter have reported instances of tailgating. Which of the following could be implemented to prevent this security concern?

A. Proximity readers
B. Mantraps
C. Video surveillance
D. Biometric keypad

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A visitor plugs their laptop into the network and receives a warning about their antivirus being cutoff-ate along with various patches that are missing. The visitor is unable to access the Internet or any network resources. Which of the following is the MOST likely cause?

A. The IDS detected that the visitor's laptop did not have the right patches and updates so the DS blocked access to the network.
B. The security posture is disabled on the network but remediation must take place before access s given to the visitor on that laptop.
C. The security posture is enabled on the network and remediation must take place before access is given to the visitor on that laptop.
D. The IPS detected that the visitor's laptop did not have the right patches and updates so it revenged its access to the network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which of the following is a detective security control?

A. CCTV
B. Firewall

C. Design reviews
D. Bollards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Which of the following identifies some of the running services on a system?

A. Determine open ports
B. Review baseline reporting
C. Review honey pot logs
D. Risk calculation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A security administrator is tasked with revoking the access of a terminated employee. Which of he following account policies MUST be enacted to ensure the employee no longer has access to the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A company needs to be able to prevent entry, at all times, to a highly sensitive area inside a public building. In order to ensure the BEST type of physical security, which of the following should be implemented?

A. Intercom system
B. Video surveillance
C. Nightly guards
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Which of the following would provide the MOST reliable proof that a datacenter was accessed at Certain time of day?

A. Video surveillance
B. Security log
C. Entry log
D. Proximity readers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following should be performed on a computer to protect the operating system from malicious software? (Select TWO).

A. Disable unused services
B. Update NIDS signatures
C. Update HIPS signatures
D. Disable DEP settings
E. Install a perimeter firewall

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
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 not consideration while evaluating this product?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
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: (none)
Explanation

Explanation/Reference:

QUESTION 158
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: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following describes a passive attempt to identify weaknesses?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
An existing application has never been assessed from a security perspective. Which of the following is the BEST assessment technique in order to identify the application's security posture?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 161
An administrator identifies a security issue on the corporate web server, but does not attempt to exploit it. Which of the following describes what the administrator has done?

A. Vulnerability scan
B. Penetration test
C. Social engineering
D. Risk mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
The server log shows 25 SSH login sessions per hour. However, it is a large company and the administrator does not know if this is normal behavior or if the network is under attack. Where hold the administrator look to determine if this is normal behavior?

A. Change management
B. Code review
C. Baseline reporting
D. Security policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Users of specific systems are reporting that their data has been corrupted. After a recent patch update to those systems, the users are still reporting issues of data being corrupt. Which of the following assessment techniques need to be performed to identify the issue?

A. Hardware baseline review
B. Vulnerability scan
C. Data integrity check
D. Penetration testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164

Which of the following is used when performing a qualitative risk analysis?

A. Exploit probability
B. Judgment
C. Threat frequency
D. Asset value

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment.
B. Business impact analysis.
C. Risk management framework.
D. Quantitative risk assessment.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
A security administrator wants to know which systems are more susceptible to an attack compared to other systems on the network. Which of the following assessment tools would be MOST effective?

A. Network design review
B. Vulnerability scanner
C. Baseline review
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
Which of the following is a management control type?

A. Vulnerability scanning
B. Least privilege implementation
C. Baseline configuration development
D. Session locks

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 168
Which of the following devices would allow a technician to view IP headers on a data packet?

A. NIDS
B. Protocol analyzer
C. VPN switch
D. Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
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: (none)
Explanation

Explanation/Reference:

QUESTION 170
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: (none)
Explanation

Explanation/Reference:

QUESTION 171
Penetration testing should only be used during controlled conditions with express consent of the system owner because:

A. White box penetration testing cannot identify zero day exploits.

B. Vulnerability scanners can cause massive network flooding during risk assessments.
C. Penetration testing passively tests policy controls and can identify vulnerabilities.
D. Penetration testing actively tests security controls and can cause system instability.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Topic 4, Application, Data and Host Security

QUESTION 172
Which of the following security practices should occur initially in software development?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
A penetration test shows that almost all database servers were able to be compromised through default database user account with the default password. Which of the following is MOST like issuing from the operational procedures?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
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: (none)
Explanation

Explanation/Reference:

QUESTION 175
Which of the following allows an attacker to identify vulnerabilities within a closed source software application?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following would an administrator do to ensure that an application is secure and all necessary services are disabled?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A security administrator ensures that certain characters and commands entered on a web server re not interpreted as legitimate data and not passed on to backend servers. This is an example of which of the following?

A. Error and exception handling
B. Input validation
C. Determining attack surface
D. Data execution prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A business-critical application will be installed on an Internet facing server. Which of the following s the BEST security control that should be performed in conjunction with updating the application
o the MOST current version?

A. The firewall should be configured to allow the application to auto-update.
B. The firewall should be configured to prevent the application from auto-updating.
C. A port scan should be run against the application's server.
D. Vendor-provided hardening documentation should be reviewed and applied.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following has a programmer MOST likely failed to consider if a user entering improper input is able to crash a program?

A. SDLM
B. CRC
C. Data formatting
D. Error handling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
Which of the following is the MOST efficient way to combat operating system vulnerabilities?

A. Anti-spam
B. Locking cabinets
C. Screen locks
D. Patch management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following is a hardening step of an application during the SDLC?

A. Disabling unnecessary accounts
B. Application patch management schedule
C. Secure coding concepts
D. Disabling unnecessary services

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
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: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following should be performed if a smart phone 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: (none)
Explanation

Explanation/Reference:

QUESTION 184
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: (none)
Explanation

Explanation/Reference:

QUESTION 185
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: (none)
Explanation

Explanation/Reference:

QUESTION 186
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: (none)
Explanation

Explanation/Reference:

QUESTION 187
A security administrator has been receiving support tickets for unwanted windows appearing on ser's workstations. Which of the following can the administrator implement to help prevent this from happening?

A. Pop-up blockers
B. Screen locks
C. Host-based firewalls
D. Antivirus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
Which of the following would an administrator apply to mobile devices to BEST ensure the confidentiality of data?

A. Screen locks
B. Device encryption
C. Remote sanitization
D. Antivirus software

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which of the following is a security vulnerability that can be disabled for mobile device users?

A. Group policy
B. Remote wipe
C. GPS tracking
D. Pop-up blockers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Which of the following software should a security administrator implement if several users are tating that they are receiving unwanted email containing advertisements?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
An employee stores their list of passwords in a spreadsheet on their local desktop hard drive. which of the following encryption types would protect this information from disclosure if lost or stolen?

A. Database
B. Removable media
C. File and folder level
D. Mobile device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A company has remote workers with laptops that house sensitive data. Which of the following can e implemented to recover the laptops if they are lost?

A. GPS tracking
B. Whole disk encryption
C. Remote sanitation
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
When decommissioning old hard drives, which of the following is the FIRST thing a security engineer should do?

A. Perform bit level erasure or overwrite
B. Flash the hard drive firmware
C. Format the drive with NTFS
D. Use a waste disposal facility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following devices provides storage for RSA or asymmetric keys and may assist in ser 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: (none)
Explanation

Explanation/Reference:

QUESTION 195
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: (none)
Explanation

Explanation/Reference:

QUESTION 196
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: (none)
Explanation

Explanation/Reference:

QUESTION 197
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: (none)
Explanation

Explanation/Reference:

QUESTION 198
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: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which of the following are the BEST reasons to use an HSM? (Select TWO).

A. Encrypt the CPU L2 cache
B. Recover keys
C. Generate keys
D. Transfer keys to the CPU

E. Store keys

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
A company needs to reduce the risk of employees emailing confidential data outside of the company. Which of the following describes an applicable security control to mitigate this threat?

A. Install a network-based DLP device
B. Prevent the use of USB drives
C. Implement transport encryption
D. Configure the firewall to block port 110

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Exam B

QUESTION 1
Which of the following can cause hardware based drive encryption to see slower deployment?

A. A lack of management software
B. USB removable drive encryption
C. Role/rule-based access control
D. Multifactor authentication with smart cards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is the MOST secure way of storing keys or digital certificates used for decryption/ encryption of SSL sessions?

A. Database
B. HSM
C. Key escrow
D. Hard drive

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following is a removable device that may be used to encrypt in a high availability clustered environment?

A. Cloud computer
B. Hsm
C. Biometrics
D. Tpm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A security administrator is implementing a solution that encrypts an employee's newly purchased atop but does not require the company to purchase additional hardware or software. Which of he following could be used to meet this requirement?

A. Mobile device encryption

B. HSM
C. TPM
D. USB encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
During incident response, which of the following procedures would identify evidence tampering by outside entities?

A. Hard drive hashing
B. Annualized loss expectancy
C. Developing audit logs
D. Tracking man hours and incident expenses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which of the following protocols only encrypts password packets from client to server?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following methods of access, authentication, and authorization is the MOST secure y default?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following uses tickets to identify users to the network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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: (none)
Explanation

Explanation/Reference:

QUESTION 10
When granting access, which of the following protocols uses multiple-challenge responses for authentication, authorization and audit?

A. Tacacs
B. Tacacs+
C. Ldap
D. Radius

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A security administrator is setting up a corporate wireless network using WPA2 with CCMP but does not want to use PSK for authentication. Which of the following could be used to support 02.1 x authentications?

A. LDAP
B. RADIUS
C. Kerberos

D. Smart card

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following authentication services would be used to authenticate users trying to access a network device?

A. SSH
B. SNMPv3
C. TACACS+
D. TELNET

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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: (none)
Explanation

Explanation/Reference:

QUESTION 14
Centrally authenticating multiple systems and applications against a federated user database is n Example of:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

A Human Resource manager is assigning access to users in their specific department performing he 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. Newer: a

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
The security administrator often observes that an employee who entered the datacenter does not match the owner of the PIN that was entered into the keypad. Which of the following would BEST prevent this situation?

A. Multifactor authentication
B. Username and password
C. Mandatory access control
D. Biometrics

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18
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: (none)
Explanation

Explanation/Reference:

QUESTION 19
A security administrator wants to prevent users in sales from accessing their servers after 6:00 .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: (none)
Explanation

Explanation/Reference:

QUESTION 20
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: (none)
Explanation

Explanation/Reference:

QUESTION 21
A security administrator with full administrative rights on the network is forced to change roles on 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: (none)
Explanation

Explanation/Reference:

QUESTION 22

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: (none)
Explanation

Explanation/Reference:

QUESTION 23
A proximity card reader is used to test which of the following aspects of human authentication?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following would be considered multifactor authentication?

A. Pin number and a smart card
B. ACL entry and a pin number
C. Username and password
D. Common access card

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is a form of photo identification used to gain access into a secure location?

A. Token
B. CAC
C. DAC
D. Biometrics

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 26
Which of the following is a trusted OS implementation used to prevent malicious or suspicious code from executing on Linux and UNIX platforms?

A. SELinux
B. vmlinuz
C. System File Checker (SFC)
D. Tripwire

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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 expiration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following is an example of requiring users to have a password of 16 characters or ore?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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: (none)
Explanation

Explanation/Reference:

QUESTION 30
Employees are required to come up with a pass phrase of at least 15 characters to access the operate network. Which of the following account policies does this exemplify?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
An administrator has implemented a policy that passwords expire after 60 days and cannot match heir last six previously used passwords. Users are bypassing this policy by immediately changing heir passwords six times and then back to the original password. Which of the following can the administrator MOST easily employ to prevent this unsecured practice, with the least administrative Effort?

A. Create a policy that passwords must be no less than ten characters.
B. Monitor user accounts and change passwords of users found to be doing this.
C. Create a policy that passwords cannot be changed more than once a day.
D. Monitor user accounts and lock user accounts that are changing passwords excessively.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following MUST be implemented in conjunction with password history, to prevent a ser from re-using the same password?

A. Maximum age time
B. Lockout time
C. Minimum age time
D. Expiration time

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following represents the complexity of a password policy which enforces lower case password using letters from 'a' through 'z' where 'n' is the password length?

A. n26
B. 2n * 26
C. 26n
D. n2 * 26

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Topic 6, Cryptography

QUESTION 34
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 s lost
D. Maintains a secured copy of a user's public key in order to improve network performance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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: (none)
Explanation

Explanation/Reference:

QUESTION 36
The fundamental difference between symmetric and asymmetric key cryptographic systems is hat 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: (none)
Explanation

Explanation/Reference:

QUESTION 37
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: (none)
Explanation

Explanation/Reference:

QUESTION 38
When a user first moves into their residence, the user receives a key that unlocks and locks their front door. This key is only given to them but may be shared with others they trust. Which of the following cryptography concepts is illustrated in the example above?

A. Asymmetric key sharing
B. Exchange of digital signatures
C. Key escrow exchange
D. Symmetric key sharing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following cryptography types provides the same level of security but uses smaller ey sizes and less computational resources than logarithms which are calculated against a finite field?

A. Elliptical curve
B. Diffie-Hellman
C. Quantum
D. El Gamal

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
The BEST way to protect the confidentiality of sensitive data entered in a database table is to se:

A. Hashing.
B. Stored procedures.
C. Encryption.
D. Transaction logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
WEP is seen as an unsecured protocol based on its improper use of which of the following?

A. RC6
B. RC4
C. 3DES
D. AES

Correct Answer: B
Section: (none)
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: (none)
Explanation

Explanation/Reference:

QUESTION 43
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: (none)
Explanation

Explanation/Reference:

QUESTION 44
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: (none)
Explanation

Explanation/Reference:

QUESTION 45
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: (none)
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. passed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following does a TPM allow for?

A. Cloud computing
B. Full disk encryption
C. Application hardening
D. Input validation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
The company encryption policy requires all encryption algorithms used on the corporate network to have a key length of 128-bits. Which of the following algorithms would adhere to company policy?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
The security administrator wants to ensure messages traveling between point A and point B are encrypted and authenticated. Which of the following accomplishes this task?

A. MD5
B. RSA
C. Diffie-Hellman
D. Whole disk encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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: (none)
Explanation

Explanation/Reference:

QUESTION 51
Where are revoked certificates stored?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the cipher text?

A. Private
B. Escrow
C. Public
D. Preshared

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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: (none)
Explanation

Explanation/Reference:

QUESTION 54
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: (none)
Explanation

Explanation/Reference:

QUESTION 55
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: (none)
Explanation

Explanation/Reference:

QUESTION 56
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: (none)
Explanation

Explanation/Reference:

QUESTION 57
The security administrator is tasked with authenticating users to access an encrypted database. Authentication takes place using PKI and the encryption of the database uses a separate cryptographic process to decrease latency. Which of the following would describe the use of encryption in this situation?

A. Private key encryption to authenticate users and private keys to encrypt the database
B. Private key encryption to authenticate users and public keys to encrypt the database

C. Public key encryption to authenticate users and public keys to encrypt the database
D. Public key encryption to authenticate users and private keys to encrypt the database

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
When a certificate issuer is not recognized by a web browser, which of the following is the MOST common reason?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is a requirement when implementing PKI if data loss is unacceptable?

A. Web of trust
B. Non-repudiation
C. Key escrow
D. Certificate revocation list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following is true about PKI? (Select TWO).

A. When encrypting a message with the public key, only the public key can decrypt it.
B. When encrypting a message with the private key, only the private key can decrypt it.
C. When encrypting a message with the public key, only the CA can decrypt it.
D. When encrypting a message with the public key, only the private key can decrypt it.
E. When encrypting a message with the private key, only the public key can decrypt it.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
The recovery agent is used to recover the:

A. root certificate.
B. key in escrow.
C. public key.
D. private key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following is true about the CRL?

A. It should be kept public
B. It signs other keys
C. It must be kept secret
D. It must be encrypted

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A file has been encrypted with an employee's private key. When the employee leaves the company, their account is deleted. Which of the following are the MOST likely outcomes? (Select TWO).

A. Recreate the former employee's account to access the file.
B. Use the recovery agent to decrypt the file.
C. Use the root user account to access the file.
D. The data is not recoverable.

E. Decrypt the file with PKI.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Topic 7, Mixed Questions

QUESTION 65
Which of the following is the BEST filtering device capable of state ful packet inspection?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
An employee's workstation is connected to the corporate LAN. Due to content filtering restrictions, the employee attaches a 3G Internet dongle to get to websites that are blocked by the corporate gateway. Which of the following BEST describes a security implication of this practice?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
In a disaster recovery situation, operations are to be moved to an alternate site. Computers and network connectivity are already present; however, production backups are several days out of date. Which of the following site types is being described?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
All of the following are valid cryptographic hash functions EXCEPT:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following PKI components identifies certificates that can no longer be trusted?

A. CRL
B. CA public key
C. Escrow
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following can prevent an unauthorized person from accessing the network by plugging into an open network jack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A digital signature provides which of the following security functions for an email message?

A. Encryption
B. Hashing
C. Input validation
D. Non-repudiation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
By default, CCMP will use which of the following to encrypt wireless transmissions?

A. RC4
B. Blowfish
C. AES
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A programmer cannot change the production system directly and must have code changes reviewed and approved by the production system manager. Which of the following describes this control type?

A. Discretionary access control
B. Separation of duties
C. Security policy
D. Job rotation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
ARP poison routing attacks are an example of which of the following?

A. Distributed Denial of Service
B. Smurf Attack
C. Man-in-the-middle
D. Vishing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company hires a security firm to assess the security of the company's network. The company does not provide the firm with any internal knowledge or documentation of the network. Which of the following should the security firm perform?

A. Black hat
B. Black box
C. Gray hat
D. Gray box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Steganography is a form of which of the following?

A. Block ciphering
B. Quantum cryptography
C. Security through obscurity
D. Asymmetric encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
In a public key infrastructure, a trusted third party is also known as which of the following?

A. Public key
B. Certificate signing request
C. Common name
D. Certificate authority

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 79
Which of the following relies on creating additional traffic to congest networks? (Select TWO).

A. Logic bomb
B. Smurf attack
C. Man-in-the-middle attack
D. DDoS
E. DNS poisoning

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following threats are specifically targeted at high profile individuals?

A. Whaling
B. Malicious insider
C. Privilege escalation
D. Shoulder surfing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following devices is MOST commonly vulnerable to bluesnarfing?

A. Mobile devices
B. Desktops
C. Digital signage
D. Ethernet jacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Which of the following application attacks typically involves entering a string of characters and bypassing input validation to display additional information?

A. Session hijacking
B. Zero day attack
C. SQL injection
D. Cross-site scripting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following features should be enabled on perimeter doors to ensure that unauthorized access cannot be gained in the event of a power outage?

A. Manual override
B. Fail closed
C. Mantrap
D. Fail open

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following is the BEST tool to use when analyzing incoming network traffic?

A. Sniffer
B. Port scanner
C. Firewall
D. Syslog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following MOST likely has its access controlled by TACACS+? (Select TWO).

A. Mobile devices
B. Active directory
C. Router
D. Switch
E. Kerberos

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Providing elastic computing resources that give a client access to more resources, allowing for distribution of large jobs across a flexible number of machines, or allowing for distributed storage of information are all hallmarks of which technology?

A. Remote access
B. Clustering
C. Cloud computing
D. IP networking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following network security techniques can be easily circumvented by using a network snuffer?

A. Disab ling the SSID broadcast
B. Enabling strong wireless encryption
C. Implementing MAC filtering on WAPs
D. Reducing the wireless power level

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following authentication services can be used to provide router commands to enforce policies?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following ports is used for telnet by default?

A. 21

B. 23
C. 25
D. 33

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following BEST describes a malicious application that attaches itself to other files?

A. Rootkits
B. Adware
C. Backdoors
D. Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
When an attack using a publicly unknown vulnerability compromises a system, it is considered to be which of the following?

A. IV attack
B. Zero day attack
C. Buffer overflow
D. Malicious insider threat

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A professor at a university is given two keys. One key unlocks a classroom door and the other locks it. The key used to lock the door is available to all other faculty. The key used to unlock the door is only given to the professor. Which of the following cryptography concepts is illustrated in the example above?

A. Key escrow exchange
B. Asymmetric key sharing
C. Exchange of digital signatures
D. Symmetric key sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following are often used to encrypt HTTP traffic? (Select TWO).

A. PAP
B. SCP
C. SHA
D. TLS
E. SSL

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following attacks targets high profile individuals?

A. Logic bomb
B. Smurf attack
C. Whaling
D. Fraggle attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A penetration tester is collecting a large amount of wireless traffic to perform an IV attack. Which of the following can be gained by doing this?

A. WPA2 shared secret
B. WPA key
C. WEP key
D. EAP-TLS private key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following allows users in offsite locations to connect securely to a corporate office?

A. Telnet

B. FTP
C. VPN
D. SNMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
On a website, which of the following protocols facilitates security for data in transit?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following security controls is the BEST mitigation method to address mobile device data theft? (Select TWO).

A. Inventory logs
B. Remote wipe
C. Device encryption
D. Host-based firewall
E. Check in and check out paperwork

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following BEST describes the purpose of fizzing?

A. To decrypt network sessions
B. To gain unauthorized access to a facility
C. To hide system or session activity
D. To discover buffer overflow vulnerabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
There are several users for a particular Human Resources database that contains PII. Which of the following principles should be applied to the users in regards to privacy of information?

A. Single sign-on
B. Least privilege
C. Time of day restrictions
D. Multifactor authentication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following would be a reason to implement DAC as an access control model?

A. Management should have access to all resources
B. An employee's security level should determine the access level
C. The owner of the data should decide who has access
D. Centrally administered roles determine who has access

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A security administrator needs to install a new switch for a conference room where two different groups will be having separate meetings. Each of the groups uses different subnets and need to have their traffic separated. Which of the following would be the SIMPLEST solution?

A. Create ACLs to deny traffic between the two networks on the switch.
B. Install a network firewall.
C. Create two VLANs on the switch.
D. Add a router to separate the two networks.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following would need to be added to a network device's configuration in order to keep track of the device's various parameters and to monitor status?

A. SNMP string

B. ACLs
C. Routing information
D. VLAN information

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A user reports the ability to access the Internet but the inability to access a certain secure website. The web browser reports the site needs to be viewed under a secure connection. Which of the following is the MOST likely cause? (Select TWO).

A. The site is using TLS instead of SSL.
B. The user is not using HTTP.
C. The site is not using URL redirection.
D. ICMP needs to be enabled.
E. The user is not using HTTPS.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following is a control that is gained by using cloud computing?

A. Data encryption
B. High availability of the data
C. Administrative control of the data
D. Physical control of the data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following is the BEST way to implement data leakage prevention? (Select TWO).

A. Installing DLP software on all computers along with the use of policy and procedures
B. Installing DLP software on all perimeter appliances and incorporating new policies and procedures
C. Securing all appliances and computers that control data going into the network along with the use of policy and procedures
D. Ensuring the antivirus, NIDS, anti-malware software, and signatures are up-to-date
E. Implementing firewall access control lists to block all incoming attachments

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A tape library containing a database with sensitive information is lost in transit to the backup location. Which of the following will prevent this media from disclosing sensitive information? (Select TWO).

A. Mobile device encryption
B. Full disk encryption
C. Database encryption
D. Discretionary access control
E. Trusted platform module

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A security administrator ensures that rights on a web server are not sufficient to allow outside users to run JavaScript commands. This is an example of which of the following?

A. Application patch management
B. Data execution prevention
C. Error and exception handling
D. Cross-site scripting prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following creates a publicly accessible network and isolates the internal private network from the Internet?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110

A security administrator is encrypting all smart phones connected to the corporate network. Which of the following could be used to meet this requirement?

A. Mobile device encryption
B. Database encryption
C. Network encryption
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Using both a username and a password is an example of:

A. biometric authentication
B. something a user knows and something a user has
C. single factor authentication
D. multifactor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which of the following password policies are designed to increase the offline password attack time? (Select TWO).

A. Password expiration
B. Password lockout time
C. Password age time
D. Password complexity
E. Password length

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
GPU processing power is a mitigating factor for which of the following security concerns?

A. Password complexity
B. Cloud computing
C. Biometrics
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
Which of the following can the security administrator implement to BEST prevent laptop device theft?

A. Device encryption
B. Cable locks
C. GPS tracking
D. CCTV

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
The pharmacy has paper forms ready to use if the computer systems are unavailable. Which of the following has been addressed?

A. Continuity of operations
B. Single point of failure
C. Disaster recovery
D. Business process reengineering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following causes an issue when acquiring an image that occurs when a server hard drive is forensically examined?

A. Servers often use RAID
B. Servers contain sensitive information
C. Servers cannot be powered down
D. Servers often use file systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Which of the following provides the BEST metric for determining the effectiveness of a Continuity of Operations

Plan or Disaster Recovery Plan?

A. Average downtime
B. Mean time between failures
C. Mean time to restore
D. Average uptime

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following is the correct formula for calculating mean time to restore (MTTR)?

A. MTTR = (time of fail) / (time of restore)
B. MTTR = (time of fail) # (time of restore)
C. MTTR = (time of restore) # (time of fail)
D. MTTR = (time of restore) x (time of fail)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
The corporate NIDS keeps track of how each program acts and will alert the security administrator if it starts acting in a suspicious manner. Which of the following describes how the NIDS I functioning?

A. Behavior based
B. Signature based
C. Host based
D. Network Access Control (NAC) based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Pete, a security technician, has chosen IPSec for remote access VPN connections for company telecommuters. Which of the following combinations would be BEST for Pete to use to secure this connection?

A. Transport mode, ESP
B. Transport mode, AH
C. Tunnel mode, AH
D. Tunnel mode, ESP

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Matt, a security administrator, is using AES. Which of the following cipher types is used by AES?

A. Block
B. Fourier
C. Stream
D. Turing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following forensic artifacts is MOST volatile?

A. CD-ROM
B. File system
C. Random access memory
D. Network topology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following protocols can Sara, a security administrator, use to implement security at the lowest OSI layer?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Which of the following protocols uses UDP port 69 by default?

A. Kerberos

B. TFTP
C. SSH
D. DNS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
After completing a forensic image of a hard drive, which of the following can Jane, a security technician, use to confirm data integrity?

A. Chain of custody
B. Image compression
C. AES256 encryption
D. SHA512 hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following can Matt, a security administrator, use to provide integrity verification when storing data?

A. Encryption
B. Hashing
C. PKI
D. ACL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following is an example of implementing security using the least privilege principle?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
The decision to build a redundant datacenter MOST likely came from which of the following?

A. Application performance monitoring
B. Utilities cost analysis
C. Business impact analysis
D. Security procedures review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Sara and Pete are unauthorized system attackers that may be able to remotely destroy critical equipment in a datacenter if they gain control over which of the following systems?

A. Physical access control
B. Video surveillance
C. HVAC
D. Packet sniffer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
In high traffic areas, Jane and Pete, security guards, need to be MOST concerned about which of the following attacks?

A. War driving
B. Blue jacking
C. Shoulder surfing
D. Tailgating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Which of the following BEST describes an attack whereby unsolicited messages are sent to nearby mobile devices?

A. Smurf attack
B. Bluejacking

C. Bluesnarfing
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Which of the following network ACL entries BEST represents the concept of implicit deny?

A. Deny UDP any
B. Deny TCP any
C. Deny ANY any
D. Deny FTP any

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following protocols assists in identifying Pete, a user, by the generation of a key, to establish a secure session for command line administration of a computer?

A. SFTP
B. FTP
C. SSH
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Which of the following is a major risk for Matt, a security administrator, to consider in regards to cloud computing?

A. Loss of physical control over data
B. Increased complexity of qualitative risk assessments
C. Smaller attack surface
D. Data labeling challenges

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Matt, a security administrator, performs various audits of a specific system after an attack. Which of the following BEST describes this type of risk mitigation?

A. Change management
B. Incident management
C. User training
D. New policy implementation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following is the MOST appropriate risk mitigation strategy for Sara, a security administrator, to use in order to identify an unauthorized administrative account?

A. Change management
B. Incident management
C. Routine audits of system logs
D. User's rights and permissions review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following would Jane, a security administrator, MOST likely look for during a vulnerability assessment?

A. Ability to gain administrative access to various systems
B. Identify lack of security controls
C. Exploit vulnerabilities
D. Actively test security controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which of the following will contain a list of unassigned public IP addresses?

A. TCP port
B. 802.1x

C. Loop protector
D. Firewall rule

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
The MAIN difference between qualitative and quantitative risk assessment is:

A. Quantitative is based on the number of assets while qualitative is based on the type of asset.
B. Qualitative is used in small companies of 100 employees or less while quantitative is used in larger companies of 100 employees or more.
C. Quantitative must be approved by senior management while qualitative is used within departments without specific approval.
D. Quantitative is based on hard numbers while qualitative is based on subjective ranking.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following attacks involves sending unsolicited contact information to Bluetooth devices configured in discover mode?

A. Impersonation
B. Blue jacking
C. War driving
D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following assessments is directed towards exploiting successive vulnerabilities to bypass security controls?

A. Vulnerability scanning
B. Penetration testing
C. Port scanning
D. Physical lock testing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following is the technical implementation of a security policy?

A. VLAN
B. Flood guards
C. Cloud computing
D. Firewall rules

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following can Mike, a security technician, use to prevent numerous SYN packets from being accepted by a device?

A. VLAN management
B. Transport encryption
C. Implicit deny
D. Flood guards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following can Jane, a security technician, use to stop malicious traffic from affecting the company servers?

A. NIDS
B. Protocol analyzers
C. Snuffers
D. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which of the following tools allows a security company to identify the latest unknown attacks utilized by attackers?

A. IDS

B. Honey pots
C. Port scanners
D. Code reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
If continuity plans are not regularly exercised, which of the following aspects of business continuity planning are often overlooked until a disaster occurs?

A. Zero day exploits
B. Succession planning
C. Tracking of man hours
D. Single points of failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Large, partially self-governing, collection of hosts executing instructions for a specific purpose is an example of which type of malware?

A. Virus
B. Worm
C. Trojan
D. Botnet

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
Which of the following attacks is BEST described as an attempt to convince Matt, an authorized user, to provide information that can be used to defeat technical security controls?

A. Shoulder surfing
B. Tailgating
C. Impersonation
D. Packet sniffing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Randomly attempting to connect to wireless network access points and documenting the locations of accessible networks is known as which of the following?

A. Packet sniffing
B. War chalking
C. Evil twin
D. War driving

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which of the following should Sara, a security technician, check regularly to avoid using compromised certificates?

A. CRL
B. PKI
C. Key escrow
D. CA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Matt, a user, was able to access a system when he arrived to work at 5:45 a.m. Just before Matt left at 6:30 p.m., he was unable to access the same system, even though he could ping the system. In a Kerberos realm, which of the following is the MOST likely reason for this?

A. Matt's ticket has expired.
B. The system has lost network connectivity.
C. The CA issued a new CRL.
D. The authentication server is down.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Pete, a security administrator, is considering using TACACS+. Which of the following is a reason to use TACACS+ over RADIUS?

A. Combines authentication and authorization
B. Encryption of all data between client and server
C. TACACS+ uses the UDP protocol
D. TACACS+ has less attribute-value pairs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A company is looking at various solutions to manage their large datacenter. The company has a lot of sensitive data on unreliable systems. Which of the following can Matt, a security technician, Use to allow the company to minimize their footprint?

A. Infrastructure as a Service
B. Implement a NAC server
C. Software as a Service
D. Create a new DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A hard drive of a terminated employee has been encrypted with full disk encryption, and Sara, a technician, is not able to decrypt the data. Which of the following ensures that, in the future, Sara will be able to decrypt this information?

A. Certificate authority
B. Key escrow
C. Public key
D. Passphrase

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following is true about the private key in a PKI?

A. It is used by the recovery agent to generate a lost public key
B. It is used by the CA to validate a user's identity
C. It is used to decrypt the email hash in signed emails
D. It is used to encrypt the email hash in signed emails

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
Which of the following is an example of authentication using something Sara, a user, has and something she is?

A. Username and PIN
B. Token and PIN
C. Password and retina scan
D. Token and fingerprint scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
Which of the following allows Jane, a security administrator, to divide a network into multiple zones? (Select TWO).

A. PAT
B. EIGRP
C. VLAN
D. NAT
E. Subnetting

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following attacks is MOST likely prevented when a website does not allow the '<' character as the input in a web form field?

A. Integer overflow
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following must Pete, a security administrator, install on a flash drive to allow for portable drive data confidentiality?

A. USB encrypt or
B. Hardware write lock
C. USB extension cable
D. Ext2 file system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
An online banking portal is not accessible by customers during a holiday season. Sara and Pete, network administrators, notice sustained, extremely high network traffic being directed towards the web interface of the banking portal from various external networks. Which of the following BEST describes what is occurring?

A. X-Mass attack
B. DDoS attack
C. DNS poisoning
D. DOS attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
While chatting with friends over IM, Matt, a user, receives numerous instant messages from strangers advertising products or trying to send files. Which of the following BEST describes the threat?

A. Spear phasing
B. Spam
C. Spim
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Which of the following is the MOST likely implication of a corporate firewall rule that allows TCP port 22 from any internal IP to any external site?

A. Data loss can occur as an SSH tunnel may be established to home PCs.
B. NAT of external websites to the internal network will be limited to TCP port 22 only.

C. Host based firewalls may crash due to protocol compatibility issues.
D. IPSec VPN access for home users will be limited to TCP port 22 only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Jane, a network administrator, changes the default usernames and passwords on an 802.11n router. This is an example of which of the following network management controls?

A. System hardening
B. Rule-based management
C. Network separation
D. VLAN management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
Jane, a security technician, needs to transfer files. Which of the following is the file transfer function that utilizes the MOST secure form of data transport?

A. TFTP
B. FTP active
C. FTP passive
D. SFTP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Which of the following, when used in conjunction with software-based encryption, enhances platform authentication by storing unique RSA keys and providing crypto processing?

A. LDAP
B. TPM
C. Kerberos
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Which of the following exploitation types involves injection of pseudo-random data in order to crash or provide unexpected results from an application?

A. Cross-site forgery
B. Brute force attack
C. Cross-site scripting
D. Fizzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
Which of the following ports would Sara, a security administrator, need to be open to allow TFTP by default?

A. 69
B. 110
C. 137
D. 339

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Pete, a customer, has called a company to report that all of his computers are displaying a rival company's website when Pete types the correct URL into the browser. All of the other websites he visits work correctly and other customers are not having this issue. Which of the following has MOST likely occurred?

A. The company's website has a misconfigured firewall.
B. Pete has a virus outbreak.
C. Pete's DNS has been poisoned.
D. The company's website has been attacked by the rival company.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Jane, a system administrator, sees a firewall rule that applies to 10.4.4.58/27. Which of the following IP address ranges are encompassed by this rule?

A. 10.4.4.27, 10.4.4.58

B. 10.4.4.32, 10.4.4.63
C. 10.4.4.58, 10.4.4.89
D. 10.4.4.58, 10.4.4.127

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which of the following would be implemented if Jane, a security administrator, wants a door to electronically unlock when certain employees need access to a location?

A. Device locks
B. Video surveillance
C. Mantraps
D. Proximity readers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which of the following is considered strong authentication?

A. Trusted OS
B. Smart card
C. Biometrics
D. Multifactor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Which of the following is an example of a smart card?

A. PIV
B. MAC
C. One-time passwords
D. Tokens

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which of the following is a security best practice that allows Pete, a user, to have one ID and password for all systems?

A. SSO
B. PIV
C. Trusted OS
D. Token

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following is an example of the type of access control methodology provided on Windows systems by default?

A. Single Sign-On
B. Discretionary Access Control (DAC)
C. Mandatory Access Control (MAC)
D. Rule based Access Control (RBAC)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
Which of the following is the MOST thorough way to discover software vulnerabilities after its release?

A. Baseline reporting
B. Design review
C. Code review
D. Fuzzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following is the way Pete, a security administrator, can actively test security controls on a system?

A. White box testing
B. Port scanning
C. Penetration testing

D. Vulnerability scanning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following is another name for fizzing third party proprietary software?

A. Grey box testing
B. Black box testing
C. White box testing
D. Blue jacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which of the following application attacks can be used against Active Directory based systems?

A. XML injection
B. SQL injection
C. LDAP injection
D. Malicious add-ons

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following is a security best practice that Jane, a security technician, would implement before placing a new server online?

A. On-demand computing
B. Host software base lining
C. Virtualization
D. Code review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180

Which of the following software types can Sara, a security technician, use to protect against no malicious but irritating malware?

A. Pop-up blockers
B. Antivirus
C. Host-based firewalls
D. Anti-spy ware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following is the MOST common security issue on web-based applications?

A. Hardware security
B. Transport layer security
C. Input validation
D. Fizzing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following can cause data loss from web based applications?

A. Device encryption
B. Poor error handling
C. Application hardening
D. XML

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following is a preventative physical security control?

A. CCTV
B. Armed guard
C. Proper lighting
D. Access list

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 184
Matt, a security administrator, is considering using cloud computing. Which of the following security concerns is MOST prominent when utilizing cloud computing service providers?

A. Video surveillance
B. Mobile device access
C. Removable storage media
D. Blended systems and data

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Which of the following is a security control that can utilize a command such as 'deny ip any any'?

A. ACL
B. Content inspection
C. Network bridge
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which of the following is an account management principle for simplified user administration?

A. Ensure password complexity requirements are met.
B. Disable unused system accounts.
C. Implement access based on groups.
D. Ensure minimum password length is acquired.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
In which of the following locations can password complexity be enforced via group policy?

A. Domain controllers

B. Local SAM databases
C. ACLs
D. NAC servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A Black Box assessment of an application is one where Sara, the security assessor, has:

A. access to the source code and the development documentation
B. no access to the application's source code and development documentation
C. access to the UAT documentation but not the source code
D. no access to the source code but access to the development documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
Which of the following security controls should Pete, the security administrator, implement to prevent server administrators from accessing information stored within an application on a server?

A. File encryption
B. Full disk encryption
C. Change management
D. Implicit deny

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Which of the following can Pete, a security technician, deploy to provide secure tunneling services?

A. IPv6
B. DNSSEC
C. SNMPv2
D. SNMPv3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
Which of the following is a reason Pete, a security administrator, would implement Kerberos over local system authentication?

A. Authentication to multiple devices
B. Centralized file integrity protection
C. Non-repudiation
D. Greater password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
Which of the following is Pete, a security technician, MOST likely to use to secure the creation of cryptographic keys?

A. Common access card
B. Hashing algorithm
C. Trusted platform module
D. One-time pad

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
Which of the following is MOST likely to reduce the threat of a zero day vulnerability?

A. Patch management
B. Network-based intrusion detection system
C. Disabling unnecessary services
D. Host-based intrusion detection system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following has the capability to perform onboard cryptographic functions?

A. Smartcard
B. ACL
C. RFID badge

D. Proximity badge

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Matt, a security administrator, discovers that Server1 and Server2 have been compromised, and then he observes unauthorized outgoing connections from Server1 to Server2. On Server1 there is an executable named tcpdump and several files that appear to be network dump files. Finally, there are unauthorized transactions in the database on Server2. Which of the following has MOST likely occurred?

A. A logic bomb has been installed on Server1.
B. A backdoor has been installed on Server2.
C. A replay attack has been used against Server2.
D. A botnet command and control has been installed on Server1.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which of the following is MOST relevant for Jane, a security administrator, to use when investigating a SQL injection attack?

A. Stored procedures
B. Header manipulation
C. Malformed frames
D. Java byte code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
Pete, a system administrator, was recently laid off for compromising various accounting systems within the company. A few months later, the finance department reported their applications were not working correctly. Upon further investigation, it was determined that unauthorized accounting software was installed onto a financial system and several application exploits existed within that system. This is an example of which of the following?

A. Rootkit
B. Logic bomb
C. Worm
D. Trojan horse

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
During a company's relocation, Sara, a security administrator, notices that several hard copies of company directories are being thrown away in public dumpsters. Which of the following attacks is the company vulnerable to without the proper user training and awareness?

A. Hoaxes
B. Pharming
C. Social engineering
D. Brute force

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Matt, a security administrator, notices an unauthorized vehicle roaming the area on company grounds. Matt verifies that all network connectivity is up and running and that no unauthorized wireless devices are being used to authenticate other devices; however, he does notice an unusual spike in bandwidth usage. This is an example of which of the following attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Exam C

QUESTION 1
A new product is being evaluated by the security team. Which of the following would take financial and business impacts into consideration if this product was likely to be purchased for large scale use?

A. Risk assessment
B. Strength of security controls
C. Application vulnerability
D. Technical threat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Jane, a security administrator, needs to make a change in the network to accommodate a new remote location. The new location will be connected by a serial interface, off the main router, through a commercial circuit. This remote site will also have traffic completely separated from all other traffic. Which of the following design elements will Jane need to implement to accommodate the new location?

A. VLANs need to be added on the switch but not the router.
B. NAT needs to be re-configured to allow the remote location.
C. The current IP scheme needs to be submitted.
D. The switch needs to be virtualized and a new DMZ needs to be created.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Matt, a security administrator, has recently performed a detailed datacenter inventory of all hardware and software. This analysis has resulted in identifying a lot of wasted resources. Which of the following design elements would eliminate the wasted resources and improve the datacenter's footprint?

A. NAC
B. Virtualization
C. Remote access implementation
D. Hosted IP Centrex

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Pete, a user, reports that after a recent business trip, his laptop started having performance issues and unauthorized emails have been sent out from the laptop. Which of the following will resolve this issue?

A. Updating Pete's laptop with current antivirus
B. Updating the anti-spam application on the laptop
C. Installing a new pop-up blocker
D. Updating Pete's digital signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
When WPA is implemented using PSK by Pete, a security administrator, which of the following authentication types is he using?

A. MD5
B. LEAP
C. SHA
D. TKIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
If Jane, a security administrator, is reviewing a verified JPEG's metadata and hash against an unverified copy of the graphic, which of the following is she looking for?

A. Steganography
B. Chain of custody
C. Digital signatures
D. Whole disk encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following technologies is often used by attackers to hide the origin of an attack?

A. Open proxy
B. Load balancer
C. Flood guard
D. URL filtering

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8
Which of the following is susceptible to reverse lookup attacks if not configured properly?

A. SSL
B. IPSec
C. ICMP
D. DNS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following are the two basic components upon which cryptography relies?

A. PKI and keys
B. Algorithms and key escrow
C. Key escrow and PKI
D. Algorithms and keys

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following should Jane, a security administrator, check for when conducting a wireless audit? (Select TWO).

A. Open relays
B. Antenna placement
C. Encryption of wireless traffic
D. URL filtering
E. Open proxies

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following passwords have the MOST similar key space? (Select TWO).

A. AnDwWe9
B. check123
C. Mypassword!2~
D. C0mPTIA
E. 5938472938193859392

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Jane, the company's Chief Information Officer (CIO), contacts the security administrator about an email asking for money in order to receive the key that would decrypt the source code that the attacker encrypted. Which of the following malware types is this MOST likely to be in this situation?

A. Worm
B. Virus
C. Spy ware
D. Ransom ware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Matt, a security engineer, working at a public CA is implementing and installing a new CRL. Where should he logically place the server?

A. On a wireless network
B. Inside the DMZ
C. On an non-routable network
D. On a secure internal network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Jane, a security engineer, is deploying a new CA. Which of the following is the BEST strategy for the root CA after deploying an intermediate trusted CA?

A. It should be placed outside of the firewall.
B. It should be placed in the DMZ.
C. It should be placed within an internal network.
D. It should be shut down and kept in a secure location.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Matt, a security administrator, has installed a new server and has asked a network engineer to place the server within VLAN 100. This server can be reached from the Internet, but Matt is unable to connect from the server to internal company resources. Which of the following is the MOST likely cause?

A. The server is connected with a crossover cable.
B. VLAN 100 does not have a default route.
C. The server is in the DMZ.
D. VLAN 100 is on the internal network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Sara, a security administrator, is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string: 'or 1 ==1 -Which of the following attacks is occurring?

A. Cross-site scripting
B. XML injection
C. Buffer overflow
D. SQL injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Pete, a security administrator, is analyzing the packet capture from an IDS triggered filter. The packet capture shows the following string: <script>source=http://www.evilsite.co/evil.js</script> Which of the following attacks is occurring?

A. SQL injection
B. Redirection attack
C. Cross-site scripting
D. XML injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following is true when Sara, a user, browsing to an HTTPS site receives the message: 'The site's certificate is not trusted'?

A. The certificate has expired and was not renewed.
B. The CA is not in the browser's root authority list.
C. The intermediate CA was taken offline.
D. The CA is not in the default CRL.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following is true when Sara, a user, browsing to an HTTPS site receives the message: 'Site name mismatch'?

A. The certificate CN is different from the site DNS A record.
B. The CA DNS name is different from the root certificate CN.
C. The certificate was issued by the intermediate CA and not by the root CA.
D. The certificate file name is different from the certificate CN.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Pete, a security administrator, needs to implement a wireless system that will only be available within a building. Which of the following configurations can Pete modify to achieve this? (Select TWO).

A. Proper AP placement
B. Disable SSID broadcasting
C. Use CCMP
D. Enable MAC filtering
E. Reduce the power levels

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Sara, a technician, must configure a network device to allow only certain protocols to the external servers and block requests to other internal sources. This is an example of a:

A. demilitarized zone

B. load balancer
C. layer 2 switch
D. stateful firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Which of the following protocols should Pete, a security administrator, use to ensure that the data remains encrypted during transport over the Internet? (Select THREE).

A. TLS
B. SSL
C. FTP
D. SSH
E. HTTP
F. TFTP

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Pete, a user, wishes to encrypt only certain files and folders within a partition. Which of the following methods should Matt, a technician, recommend?

A. EFS
B. Partition encryption
C. Full disk
D. Bit Locker

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following can Jane, a security administrator, use to help prevent man-in-the-middle attacks?

A. HTTP
B. HTTPS
C. SFTP
D. Kerberos

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 25
Which of the following should Sara, a security administrator, implement on a mobile phone to help prevent a conversation from being captured?

A. Device encryption
B. Voice encryption
C. GPS tracking
D. Sniffer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following access control methods provides the BEST protection against attackers logging on as authorized users?

A. Require a PIV card
B. Utilize time of day restrictions
C. Implement implicit deny
D. Utilize separation of duties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following should Matt, a security technician, integrate into the fire alarm systems to help prevent a fire from spreading?

A. HVAC
B. Humidity controls
C. Video monitoring
D. Thermostats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An in-line network device examines traffic and determines that a parameter within a common protocol is well outside of expected boundaries. This is an example of which of the following?

A. Anomaly based detection
B. Behavior based detection
C. IV attack detection
D. Signature based detection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Jane, a malicious insider, obtains a copy of a virtual machine image for a server containing client financial records from the in-house virtualization cluster. Which of the following would BEST prevent Jane from accessing the client records?

A. Cloud computing
B. Separation of duties
C. Portable media encryption
D. File and folder encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following is the MOST effective method to provide security for an in-house created application during software development?

A. Third-party white box testing of the completed application before it goes live
B. Third-party black box testing of the completed application before it goes live
C. Explicitly include security gates during the SDLC
D. Ensure an application firewall protects the application

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Matt, an attacker, incorrectly submits data on a website's form and is able to determine the type of database used by the application and the SQL statements used to query that database. Which of the following is responsible for this information disclosure?

A. SQL injection
B. Fizzing
C. XSS
D. Error handling

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following describes why Sara, the sender of an email, may encrypt the email with a private key?

A. Confidentiality
B. Non-repudiation
C. Transmission speed
D. Transport encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Matt, a security technician, needs to increase his password's key space. Which of the following increases the key space of a password the MOST?

A. Letters, numbers, and special characters
B. 25 or more alpha-numeric characters
C. Two-factor authentication
D. Sequential alpha-numeric patterns

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35

Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

A. RAID
B. Clustering
C. Redundancy
D. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
An offsite location containing the necessary hardware without data redundancy would be an example of which of the following off-site contingency plans?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image
D. Interview witnesses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following is BEST described as a scenario where organizational management decides not to provide a service offering because it presents an unacceptable risk to the organization?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which of the following is the primary security reason why Pete, a security administrator, should block social networking sites in a large corporation?

A. The proxy server needs to be specially configured for all social networking sites.
B. The data traffic can cause system strain and can overwhelm the firewall rule sets.
C. The users' work productivity decreases greatly.
D. The users can unintentionally post sensitive company information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following describes the importance of enacting and maintaining a clean desk policy?

A. To ensure that data is kept on encrypted network shares
B. To avoid passwords and sensitive data from being unsecured
C. To verify that users are utilizing data storage resources
D. To guarantee that users comply with local laws and regulations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Matt, a security technician, is using TFTP. Which of the following port numbers is used for TFTP?

A. 22
B. 69
C. 80
D. 3389

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following systems implements a secure key distribution system that relies on hardcopy keys

intended for individual sessions?

A. Blowfish
B. PGP/GPG
C. One-time pads
D. PKI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following devices would Jane, a security administrator, typically use at the enclave boundary to inspect, block, and re-route network traffic for security purposes?

A. Load balancers
B. Protocol analyzers
C. Firewalls
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following devices is Pete, a security administrator, MOST likely to install to prevent malicious attacks?

A. VPN concentrator
B. Firewall
C. NIDS
D. Protocol analyzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following devices should Jane, a security administrator, use to allow secure remote network access for mobile users?

A. NIDS
B. Protocol analyzer
C. SFTP
D. VPN concentrator

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following is capable of providing the HIGHEST encryption bit strength?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following technologies is used to verify that a file was not altered?

A. RC5
B. AES
C. DES
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which of the following, when used in conjunction with software-based encryption, enhances platform authentication by storing unique RSA keys and providing crypto processing?

A. LDAP
B. TPM
C. Kerberos
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 1, Volume A

QUESTION 49
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:

QUESTION 50
Sara and Jane, users, are reporting an increase in the amount of unwanted email that they are receiving each day. Which of the following would be the BEST way to respond to this issue without creating a lot of administrative overhead?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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:

QUESTION 52
Which of the following is similar to a smurf attack, but uses UDP instead to ICMP?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Pete, a security administrator, wants to secure remote telnet services and decides to use the services over SSH. Which of the following ports should Pete allow on the firewall by default?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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:

QUESTION 55
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:

QUESTION 56
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:

QUESTION 57
Sara, a security analyst, discovers which operating systems the client devices on the network are running by only monitoring a mirror port on the router. Which of the following techniques did Sara use?

A. Active fingerprinting
B. Passive finger printing
C. Protocol analyzing
D. Network enumerating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is the BEST solution to securely administer remote servers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A company has sent all of its private keys to a third party. The third party company has created a secure list of these keys. Which of the following has just been implemented?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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:

QUESTION 61
The fundamental information security principals include confidentiality, availability and which of the following?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following risks could IT management be mitigating by removing an all-in-one device?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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:

QUESTION 64
Sara, an IT administrator, wants to protect a cluster of servers in a DMZ from zero day attacks. Which of the following would provide the BEST level of protection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following inspects traffic entering or leaving a network to look for anomalies against expected baselines?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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:

QUESTION 67
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:

QUESTION 68
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:

QUESTION 69
Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following would Pete, a security administrator, change to limit how far a wireless signal will travel?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following ports should be open in order for Sara and Pete, users, to identify websites by domain name?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Sara, an administrator, suspects a denial of service attack on the network, but does not know where the network traffic is coming from or what type of traffic it is. Which of the following would help Sara further assess the situation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Sara, a security administrator, has configured a trusted OS implementation on her servers. Which of the following controls are enacted by the trusted OS implementation?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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:

QUESTION 76
Which of the following is where an unauthorized device is found allowing access to a network?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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:

QUESTION 78
Jane's, a user, word processing software is exhibiting strange behavior, opening and closing itself at random intervals. There is no other strange behavior on the system. Which of the following would mitigate this problem in the future?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
Which of the following security concepts establishes procedures where creation and approval are performed through distinct functions?

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

D. Principle of least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
While traveling Matt, an employee, decides he would like to download some new movies onto his corporate laptop. While installing software designed to download movies from multiple computers across the Internet. Matt agrees to share portions of his hard drive. This scenario describes one of the threats involved in which of the following technologies?

A. Social networking
B. ALE
C. Cloud computing
D. P2P

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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:

QUESTION 83
Pete, a security administrator, has configured and implemented an additional public intermediate CA. Which of the following must Pete submit to the major web browser vendors in order for the certificates, signed by this intermediate, to be trusted?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
3DES is created when which of the following scenarios occurs?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following is BEST described by a scenario where organizational management chooses to implement an internal Incident Response Structure for the business?

A. Deterrence
B. Separation of duties
C. Transference
D. Mitigation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A data loss prevention strategy would MOST likely incorporate which of the following to reduce the risk associated with data loss?

A. Enforced privacy policy, encryption of VPN connections, and monitoring of communications entering the organization.
B. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications leaving the organization.
C. Enforced privacy policy, encryption of VPN connections, and monitoring of communications leaving the organization.
D. Enforced acceptable usage policy, encryption of confidential emails, and monitoring of communications entering the organization.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

In a wireless network, which of the following components could cause too much coverage, too little coverage, and interference?

A. MAC filter
B. AP power levels
C. Phones or microwaves
D. SSID broadcasts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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:

QUESTION 89
Which of the following is Jane, a security administrator, MOST likely implementing when deleting all the unneeded files and modules of a newly install application?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
The public key is used to perform which of the following? (Select THREE).

A. Validate the CRL
B. Validate the identity of an email sender
C. Encrypt messages
D. Perform key recovery
E. Decrypt messages
F. Perform key escrow

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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:

QUESTION 92
Which of the following is BEST associated with PKI?

A. Private key
B. Block ciphers
C. Stream ciphers
D. NTLMv2

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Pete, a network administrator, implements the spanning tree protocol on network switches. Which of the following issues does this address?

A. Flood guard protection
B. ARP poisoning protection
C. Loop protection
D. Trunking protection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94

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:

QUESTION 95
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:

QUESTION 96
Which of the following BEST describes a denial of service attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
The Chief Information Officer (CIO) wants to protect laptop users from zero day attacks. Which of the following would BEST achieve the CIO's goal?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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:

QUESTION 99
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:

QUESTION 100
When Pete, an employee, leaves a company, which of the following should be updated to ensure Pete's security access is reduced or eliminated?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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:

QUESTION 103
Jane, an IT security technician working at a bank, has implemented encryption between two locations. Which of the following security concepts BEST exemplifies the protection provided by this example?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following mitigates the risk of proprietary information being compromised?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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:

QUESTION 106
While Sara is logging into the server from her workstation, she notices Pete watching her enter the username and password. Which of the following social engineering attacks is Pete executing?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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:

QUESTION 108
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:

QUESTION 109
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:

QUESTION 110
Which of the following should Sara, a security technician, perform as the FIRST step when creating a disaster recovery plan for a mission critical accounting system?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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:

QUESTION 112
Which of the following is an example of authentication using something Jane, a user, has and something she knows?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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:

QUESTION 114
Which of the following activities should be completed in order to detect anomalies on a network?

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 115
Which of the following describes the ability for a third party to verify the sender or recipient of a given electronic message during authentication?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Which of the following protocols provides Pete, an administrator, with the HIGHEST level of security for device traps?

A. ICMP
B. SNMPv3
C. SSH
D. IPSec

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
Jane has a vendors server in-house for shipping and receiving. She wants to ensure that if the server goes down that the server in-house will be operational again within 24 hours. Which of the following should Jane define with the vendor?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
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:

QUESTION 119
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:

QUESTION 120
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:

QUESTION 121
Pete, a user, is having trouble dialing into the network from their house. The administrator checks the RADIUS server, the switch connected to the server, and finds that the switch lost configuration after a recent power outage. The administrator replaces the switch and is able to ping the switch, but not the RADIUS server. Which of the following is the MOST likely cause?

A. The switch needs to have QoS setup correctly.
B. Port security is not enabled on the switch.
C. VLAN mismatch is occurring.

D. The DMZ is not setup correctly

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date. Which of the following BEST describes this system type?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following would MOST likely be implemented in order to prevent employees from accessing certain websites?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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:

QUESTION 126
Sara, a security analyst, suspects that a rogue web server is running on the network. Which of the following would MOST likely be used to identify the server's IP address?

A. Port scanner
B. Telnet
C. Traceroute
D. Honeypot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following is an improved version of the LANMAN hash?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which of the following will help Matt, an administrator; mitigate the risk of static electricity?

A. Lightening rods
B. EMI shielding

C. Humidity controls
D. Temperature controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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:

QUESTION 130
A company needs to remove sensitive data from hard drives in leased computers before the computers are returned to the supplier. Which of the following is the BEST solution?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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:

QUESTION 132
Jane, a security administrator, has applied security labels to files and folders to manage and restrict access. Which of the following is Jane using?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following can Pete, an administrator, use to verify that a downloaded file was not corrupted during the transfer?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Sara, a user, on a public Wi-Fi network logs into a webmail account and is redirected to a search engine. Which of the following attacks may be occurring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
When moving from an internally controlled environment to a fully outsourced infrastructure environment, such as cloud computing, it is MOST important to:

A. Implement mandatory access controls.

B. Ensure RAID 0 is implemented on servers.
C. Impose time of day restrictions across all services
D. Encrypt all confidential data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Which of the following would help Pete, an administrator, prevent access to a rogue access point connected to a switch?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A company wants to have a backup site that is a good balance between cost and recovery time objectives. Which of the following is the BEST solution?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Jane, a user, has reported an increase in email phishing attempts. Which of the following can be implemented to mitigate the attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
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:

QUESTION 140
Which of the following is a reason why Pete, a security administrator, would implement port security?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following is the MAIN benefit of server-side versus client-side input validation?

A. Server-side input validation results in a more secure system than client-side input validation.
B. Client-side input validation can lead to local buffer overflows while server-side input validation can lead to remote buffer overflow.
C. Client-side input validation results in a more secure system than server-side input validation.
D. Server-side input validation is prone to buffer overflows while client-side input validation is not.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
In the event of a mobile device being lost or stolen, which of the following BEST protects against sensitive information leakage?

A. Cable locks
B. Remote wipe
C. Screen lock
D. Voice encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Which of the following is BEST utilized to actively test security controls on a particular system?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
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:

QUESTION 145
Which of the following implements two factor authentication based on something you know and something you have?

A. Users shall authenticate to the system via a Kerberos enabled authentication server working with an integrated PKI only.
B. The system shall require users to authenticate to the system with a combination of a password or PIN and a smartcard
C. The system shall authenticate only authorized users by fingerprint and retina scan.
D. Users shall possess a combination of 8 digit PINs and fingerprint scanners.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following attacks is characterized by Sara attempting to send an email from a Chief Information Officer's (CIO's) non-corporate email account to an IT staff member in order to have a password changed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Topic 2, Volume B

QUESTION 147
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:

QUESTION 148
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:

QUESTION 149
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:

QUESTION 150
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:

QUESTION 151
Which of the following functions of a firewall allows Pete, an administrator, to map an external service to an internal host?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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:

QUESTION 154
After setting up a root CA. which of the following can Pete, a security administrator, implement to allow intermediate CAs to handout keys and certificates?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
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
D. Sara should be given read/write access for the specific document on network share A.
E. Accounting should be given full access to network share A and read access to network share
F. Sara should be given read/write access to network share A.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
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:

QUESTION 158
Which of the following is the purpose of the spanning tree protocol?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Sara, the security engineer, has discovered that a breach is in progress on a non-production system of moderate importance. Which of the following should Sara collect FIRST?

A. Memory dump, ARP cache
B. Live system image, route table
C. Temp files, hosts file
D. Offline system image, router logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
The Chief Information Security Officer (CISO) tells the network administrator that a security company has been hired to perform a penetration test against their network. The security company asks the CISO which type of testing would be most beneficial for them. Which of the following BEST describes what the security company might do during a black box test?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
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:

QUESTION 162
Which of the following is used by Matt, a security administrator, to lower the risks associated with electrostatic discharge, corrosion, and thermal breakdown?

A. Temperature and humidity controls
B. Routine audits
C. Fire suppression and EMI shielding

D. Hot and cold aisles

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Which of the following are restricted to 64-bit block sizes? (Select TWO)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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:

QUESTION 165
The human resources department of a company has requested full access to all network resources, including those of the financial department. Jane, the administrator, denies this, citing:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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:

QUESTION 167
Which of the following security tools can Jane, an administrator, implement to mitigate the risks of theft?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
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:

QUESTION 169
Which of the following ports would be blocked if Pete, a security administrator, wants to disable FTP?

A. 21
B. 23

C. 25
D. 110

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Sara, a security administrator, suspects that a web server may be under attack. The web logs have several entries containing variations of the following entries:
'or 1=1-or1'=1-'or1=1'—
Which of the following attacks is MOST likely occurring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
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:

QUESTION 172
Which of the following practices reduces the attack surface of a wireless network? (Select TWO)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which of the following combinations represents multifactor authentication?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
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:

QUESTION 175
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:

QUESTION 176
An application programmer reports to Sara, the security administrator, that the antivirus software installed on a server is interfering with one of the production HR applications, and requests that antivirus be temporarily turned off. How should Sara respond to this request?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
Which of the following allows active exploitation of security vulnerabilities on a system or network for the purpose of determining true impact?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A packet filtering firewall can protect from which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Which of the following can Matt, an administrator, use to ensure the confidentiality of a file when it is being sent over FTP?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 180
Pete, a user, submitted a form on the Internet but received an unexpected response shown below Server Error in "/" Application Runtime error in script on asp.net version 2.0 Which of the following controls should be put in place to prevent Pete from learning this information about the web server in the future?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
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:

QUESTION 182
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:

QUESTION 183

Which of the following is a feature of Kerberos?

A. One-way encryption
B. Vendor patch management
C. Only available for Linux systems
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
An SQL injection vulnerability can be caused by which of the following?

A. Password complexity
B. Improper input validation
C. Discretionary access controls
D. Cross-site request forgery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Which of the following does Jane, a software developer, need to do after compiling the source code of a program to attest the authorship of the binary?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

A. NAT
B. Virtualization
C. NAC
D. Subnetting

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
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:

QUESTION 188
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:

QUESTION 189
Which of the following commands can Matt, an administrator, use to create a forensically sound hard drive image?

A. grep
B. dump
C. dcfldd
D. hex

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190

Which of the following technologies would allow the removal of a single point of failure?

A. Dual-homing a server
B. Clustering a SQL server
C. Adding a second VLAN to a switch
D. Assigning a second IP address to a NIC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
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:

QUESTION 192
Which of the following security tools can Jane, a security administrator, use to deter theft?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
Jane, a security administrator, has completed the imaging process for 20 computers that were deployed. The image contains the operating system and all required software. Which of the following is this an example of?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
Which of the following open standards should Pete, a security administrator, select for remote authentication of users?

A. TACACS
B. RADIUS
C. WPA2
D. RIPEMD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
Matt, a system administrator, wants to establish a nightly available SQL database. Which of the following would be implemented to eliminate a single point of failure in storage and servers?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Which of the following password policies is the MOST effective against a brute force network attack?

A. Password complexity
B. Password recovery
C. 30 day password expiration
D. Account lockout

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
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:

QUESTION 198
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:

QUESTION 199
Which of the following web application security weaknesses can be mitigated by preventing the use of HTML tags?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Exam D

QUESTION 1
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:

QUESTION 2
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:

QUESTION 3
While performing basic forensic analysis of a hard drive in Sara's, the security administrator, possession, which of the following should be verified during the analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling
B. Password policy
C. Chain of custody

D. Zero day exploits

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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:

QUESTION 6
Which of the following security controls enforces user permissions based on a job role?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following should be implemented to secure Pete's, a network administrator, day-today maintenance activities? (Select TWO).

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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:

QUESTION 9
Which of the following malware types is BEST described as protecting itself by hooking system processes and hiding its presence?

A. Botnet
B. Rootkit
C. Logic bomb
D. Virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 10
A company notices that there is a flaw in one of their proprietary programs that the company runs in-house. The flaw could cause damage to the HVAC system. Which of the following would the company transfer to an insurance company?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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:

QUESTION 12
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:

QUESTION 13
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:

QUESTION 14
The corporate NIPS requires a daily download from its vendor with updated definitions in order to block the latest attacks. Which of the following describes how the NIPS is functioning?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following are security relevant policies? (Select THREE)

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

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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:

QUESTION 17
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:

QUESTION 18
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:

QUESTION 19
Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following could Sara, an administrator, use in a workplace to remove sensitive data at rest from the premises?

A. Network sniffer
B. Personally owned devices
C. Vulnerability scanner
D. Hardware locks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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:

QUESTION 22
Traffic has stopped flowing to and from the company network after the inline IPS hardware failed. Which of the following has occurred?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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:

QUESTION 24
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:

QUESTION 25
Which of the following network devices will prevent port scans?

A. Firewall
B. Load balancers
C. NIDS
D. Sniffer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following multifactor authentication methods uses biometrics?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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:

QUESTION 28
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:

QUESTION 29
Which of the following control types is video monitoring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

A. Succession planning
B. Disaster recovery
C. Separation of duty
D. Removing single loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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:

QUESTION 32
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:

QUESTION 33
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:

QUESTION 34
Pete, a security administrator, would like to implement laptop encryption to protect data. The Chief Executive Officer (CEO) believes this will be too costly to implement and decides the company will purchase an insurance policy instead. Which of the following is this an example of?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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:

QUESTION 36
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:

QUESTION 37
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:

QUESTION 38
Matt's CRL is over six months old. Which of the following could Matt do in order to ensure he has the current

information? (Select TWO).

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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:

QUESTION 40
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:

QUESTION 41
A vulnerability has been found in a service that is unnecessary for the corporate environment. Which of the following is the BEST way to mitigate this vulnerability?

A. Issue a hotfix to lower the vulnerability risk on the network
B. Issue a group policy to disable the service on the network.

C. Issue a service pack to ensure the service is current with all available patches
D. Issue a patch to ensure the service has a lower level of risk if compromised.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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:

QUESTION 43
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:

QUESTION 44
Which of the following describes separating encryption keys into multiple parts to store with trusted third parties?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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:

QUESTION 46
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:

QUESTION 47
Which of the following should Pete, a security technician, apply to a server to BEST prevent SYN attacks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 3, Volume C

QUESTION 48
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:

QUESTION 49
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:

QUESTION 50
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:

QUESTION 51
A recent policy change requires Pete, a security administrator, to implement TLS wherever possible. Which of the following can TLS secure? (Select THREE).

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

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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:

QUESTION 53
Matt, a security analyst, discovered that a commonly used website is serving up a script that redirects users to a Questionable website. Which of the following solutions MOST likely prevents this from occurring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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:

QUESTION 55
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:

QUESTION 56
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:

QUESTION 57
Which of the following is mainly used for remote access into the network?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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:

QUESTION 59
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:

QUESTION 60
Matt, a security administrator, wants to configure all the switches and routers in the network in order to security monitor their status. Which of the following protocols would he need to configure on each device?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Jane, a security administrator, recently configured the firewall for the corporate office. Some users report that they are unable to access any resources outside of the company. Which of the following is the MOST likely reason for the lack of access?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following describes common concerns when implementing IPS?

A. Legitimate traffic will be incorrectly blocked

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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:

QUESTION 64
Which of the following utilizes the ECHO function of Internet Control Message Protocol (ICMP) to overwhelm a victim's system?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Matt, an administrator, is concerned about the wireless network being discovered by war driving. Which of the following can be done to mitigate this?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Jane, the administrator of a small company, wishes to track people who access the secured server room, which is secured only by a simple hardware key lock. Jane does not have much of a budget or the approval to make significant construction changes. Given the limitations, which of the following can she do in the meantime?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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:

QUESTION 68
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:

QUESTION 69
One of the advantages of Trusted Platform Modules (TPM) is:

A. it cannot be modified by a silent background process.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following protocols is MOST closely linked with SSL?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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:

QUESTION 72
Which of the following data center environmental controls must be property configured to prevent equipment failure from water?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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:

QUESTION 74
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:

QUESTION 75
Which of the following will require exceptions when considering the use of 802.1x port security?

A. Switches
B. Printers
C. Laptops
D. Desktops

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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:

QUESTION 77
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:

QUESTION 78
A major CA has been compromised and a new patch has been released to make necessary changes on user machines. Which of the following is likely to be updated as a part of this patch?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following uses both a public and private key?

A. RSA
B. AES
C. MD5
D. SHA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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:

QUESTION 81
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:

QUESTION 82
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:

QUESTION 83
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:

QUESTION 84
Sara, an IT manager, wants to change the firewall rules to allow RemoteOfficeB to connect to the corporate network using SSH. Which of the following rules would only allow necessary access?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following attacks is characterized by someone following a staff member who is entering a corporate facility?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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:

QUESTION 87
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:

QUESTION 88
Which of the following detection methods may generate an alert when Matt, an employee, accesses a server during non-business hours?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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:

QUESTION 90

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:

QUESTION 91
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:

QUESTION 92
Jane, a security architect, is working on setting up a secure email solution between internal employees and external customers. Which of the following would BEST meet her goal?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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:

QUESTION 94
Which of the following would Jane, a security administrator, use to encrypt transmissions from streaming video transmissions, keeping in mind that each bit must be encrypted as it comes across the network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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:

QUESTION 96
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:

QUESTION 97
Sara, a security administrator, is implementing remote management for network infrastructure using SNMP. Which of the following statements is true about SNMP?

A. Read communities allow write permissions
B. Relays mail based on domain keys and access headers
C. SNMP communities are encrypted using PKI
D. Write communities allow both read and write permissions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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:

QUESTION 99
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:

QUESTION 100
Companies allowing remote access to internal systems or systems containing sensitive data should provide access using:

A. dial-up or broadband networks using passwords.
B. wireless networks using WPA encryption.
C. VPN with two factor authentication.

D. carrier based encrypted data networks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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:

QUESTION 102
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:

QUESTION 103
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:

QUESTION 104

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following would be the BEST choice for attacking a complex password hash?

A. Man in the middle
B. Dictionary files
C. Rainbow tables
D. Brute-force intrusion

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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:

QUESTION 107
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:

QUESTION 108
Which of the following would Sara, a security administrator, implement to divert and analyze attacks?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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:

QUESTION 110
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:

QUESTION 111

After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25
B. 68
C. 80
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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:

QUESTION 113
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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:

QUESTION 115
A company wants to implement a policy that helps reduce employee stress and decrease the likelihood of security incidents caused by job dissatisfaction. Which of the following will MOST likely have a positive impact on the employee stress and job satisfaction?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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:

QUESTION 117
Sara, a user, needs to copy a file from a Linux workstation to a Linux server using the MOST secure file transfer method available. Which of the following protocols would she use?

A. SCP
B. FTP
C. SNMP
D. TFTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

A. ECC
B. RSA
C. SHA
D. 3DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
Matt, a system administrator, notices that there have been many failed login attempts to the virtual server's management interface. Which of the following would be the BEST way for him to secure the virtual server's OS?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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:

QUESTION 121
Which of the following host security procedures will facilitate in the identification of Advanced Persistent Threats (APT)?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Jane, a security technician, has been called into a meeting with the management team who has a requirement for comprehensive vetting of specialized employees as part of the hiring process. Funding and resources are not an issue since staff members are in high risk positions and have access to sensitive data. Which of the following access control types BEST meets the requirement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verily the backup datacenter is prepared for such a scenario?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
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:

QUESTION 125
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:

QUESTION 126
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:

QUESTION 127
Matt, a security administrator, wants to implement a secure wireless network. Which of the following is the MOST secure wireless protocol?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 128
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:

QUESTION 129
In order to justify the cost of a new security appliance, the administrator should do which of the following?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following is responsible for masking the activity of an on-going attack from the administrator's operating system monitoring tools?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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:

QUESTION 132
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:

QUESTION 133
Jane, an attacker, compromises a payroll system and replaces a commonly executed application with a modified version which appears to run as normal but also executes additional functions. Which of the following would BEST describe the slightly modified application?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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:

QUESTION 135
Which of the following would allow Pete, a security analyst, to assess his company's proficiency with a particular security process?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
The Chief Security Officer (CSO) informs Jane, the technician, that there is a new requirement for all data repositories where data must be encrypted when not in use. The CSO wants Jane to apply this requirement to all corporate servers. Which of the following data encryption types will BEST fill this requirement?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
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:

QUESTION 138
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:

QUESTION 139
Matt, a network engineer, is implementing a VPN solution. Which of the following can Matt use to secure the user authentication session?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/