

Comptia.Certkiller.SY0-301.v2013-11-05.by.Doc.A.447q

Number: SY0-301
Passing Score: 800
Time Limit: 120 min
File Version: 16.5



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

Exam Code: SY0-301

Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version



Sections
1. Pretest

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 5

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

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



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

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

Correct Answer: AB

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 17

By default, which of the following stops network traffic when the traffic is not identified in the firewall ruleset?

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

Correct Answer: D

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 23

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

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

Correct Answer: B

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

Webmail 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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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:
Explanation:

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:
Explanation:

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:
Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 64

Risk can be managed in the following ways EXCEPT:

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

Correct Answer: C

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 85

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

8

- 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:

Explanation:

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:

Explanation:

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:

Explanation:

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: Pretest

Explanation

Explanation/Reference:

Explanation:

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 analysis

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 91

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

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

Correct Answer: D

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 94

With which of the following is RAID MOST concerned?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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 BEST describes this type of malware?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 105

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 111

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

- A. Trojans
- B. Botnets
- C. Adware
- D. Logic bomb

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 113

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 114

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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 state 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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 121

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 127

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 128

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 130

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

- A. Interference
- B. Rogue access points
- C. IV attack
- D. Bluejacking

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 132

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 135

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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:

Explanation:

QUESTION 137

Which of the following attacks is manifested as an embedded HTML image object or JavaScript image tag in an email?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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:

Explanation:

QUESTION 139

An application log shows that the text "test; rm -rf /etc/passwd" 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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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 honeypot.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 149

A visitor plugs their laptop into the network and receives a warning about their antivirus being out- of-date 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 IDS blocked access to the network.
- B. The security posture is disabled on the network but remediation must take place before access is 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 prevented its access to the network.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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 honeypot logs
- D. Risk calculation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 152

A security administrator is tasked with revoking the access of a terminated employee. Which of the 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:

Explanation:

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:

Explanation:

QUESTION 154

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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 into 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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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 should 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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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. Fuzzing
- D. Penetration tests

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 173

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 175

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 176

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 177

A security administrator ensures that certain characters and commands entered on a web server are 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:

Explanation:

QUESTION 178

A business-critical application will be installed on an Internet facing server. Which of the following is the BEST security control that should be performed in conjunction with updating the application to 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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 183

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 187

A security administrator has been receiving support tickets for unwanted windows appearing on user'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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 190

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

QUESTION 192

A company has remote workers with laptops that house sensitive data. Which of the following can be 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:

Explanation:

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:

Explanation:

QUESTION 194

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

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

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:

Explanation:

QUESTION 201

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:

Explanation:

QUESTION 202

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:

Explanation:

QUESTION 203

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:

Explanation:

QUESTION 204

A security administrator is implementing a solution that encrypts an employee's newly purchased laptop but does not require the company to purchase additional hardware or software. Which of the 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:

Explanation:

QUESTION 205

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

- A. Hard drive hashing



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

- B. Annualized loss expectancy
- C. Developing audit logs
- D. Tracking man hours and incident expenses

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Topic 5, Access Control and Identity Management

QUESTION 206

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:

Explanation:

QUESTION 207

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 208

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

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

Correct Answer: D

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 209

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:

Explanation:

QUESTION 210

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 211

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 802.1x authentication?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. Smart card

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 212

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:

Explanation:

QUESTION 213

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:

Explanation:

QUESTION 214

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 215

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 216

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:

Explanation:

QUESTION 217

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:

Explanation:

QUESTION 218

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:

Explanation:

QUESTION 219

A security administrator wants to prevent users in sales from accessing their servers after 6:00p.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:

Explanation:

QUESTION 220

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:

Explanation:

QUESTION 221

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 222

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:

Explanation:

QUESTION 223

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:

Explanation:

QUESTION 224

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:

Explanation:

QUESTION 225

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:

Explanation:

QUESTION 226

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:

Explanation:

QUESTION 227

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:

Explanation:

QUESTION 228

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 229

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:

Explanation:

QUESTION 230

Employees are required to come up with a passphrase of at least 15 characters to access the corporate 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:

Explanation:

QUESTION 231

An administrator has implemented a policy that passwords expire after 60 days and cannot match their last six previously used passwords. Users are bypassing this policy by immediately changing their passwords six times and then back to the original password. Which of the following can the administrator MOST easily employ to prevent this unsecure 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:

Explanation:

QUESTION 232

Which of the following MUST be implemented in conjunction with password history, to prevent a user 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:

Explanation:

QUESTION 233

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. 26^n
- B. $2n * 26$
- C. $n26$
- D. $n2 * 26$

Correct Answer: A

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

Topic 6, Cryptography-The base (26) represents the total number of **choices** of characters. The exponent (n) represents the length of the password. The base is easily understood when you think of numbering systems: the base simply states the total number of **choices** of characters. Examples include base 2, base 8, base 16. Additionally, complexity is the product of 26^n . This number represents the total number of possibilities (of passwords). Finally, increasing the exponent n by 1 produces a much greater increase in complexity in comparison to increasing the base by 1. Hence the term "increases exponentially."

QUESTION 234

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

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

Correct Answer: C

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 235

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 236

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

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

Correct Answer: D

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 237

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:

Explanation:

QUESTION 238

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:

Explanation:

QUESTION 239

Which of the following cryptography types provides the same level of security but uses smaller key 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:

Explanation:

QUESTION 240

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

- A. hashing.

- B. stored procedures.
- C. encryption.
- D. transaction logs.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 241

WEP is seen as an unsecure 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:

Explanation:

QUESTION 242

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:

Explanation:

QUESTION 243

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:

Explanation:

QUESTION 244

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:

Explanation:

QUESTION 245

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:

Explanation:

QUESTION 246

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 247

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:

Explanation:

QUESTION 248

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:

Explanation:

QUESTION 249

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:

Explanation:

QUESTION 250

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:

Explanation:

QUESTION 251

Where are revoked certificates stored?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 252

Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the ciphertext?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 253

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:

Explanation:

QUESTION 254

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:

Explanation:

QUESTION 255

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:

Explanation:

QUESTION 256

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:

Explanation:

QUESTION 257

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:

Explanation:

QUESTION 258

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:

Explanation:

QUESTION 259

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:

Explanation:

QUESTION 260

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:

Explanation:

QUESTION 261

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 262

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 263

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:
Explanation:

QUESTION 264

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:
Explanation:

Topic 7, Mixed Questions

QUESTION 265

Which of the following is the BEST filtering device capable of stateful packet inspection?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 266

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:

Explanation:

QUESTION 267

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:

Explanation:

QUESTION 268

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:

Explanation:

QUESTION 269

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:

Explanation:

QUESTION 270

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:

Explanation:

QUESTION 271

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:

Explanation:

QUESTION 272

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:

Explanation:

QUESTION 273

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:

Explanation:

QUESTION 274

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:

Explanation:

QUESTION 275

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:

Explanation:

QUESTION 276

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:

Explanation:

QUESTION 277

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:

Explanation:

QUESTION 278

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:

Explanation:

QUESTION 279

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:

Explanation:

QUESTION 280

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:

Explanation:

QUESTION 281

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:

Explanation:

QUESTION 282

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:

Explanation:

QUESTION 283

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:

Explanation:

QUESTION 284

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:

Explanation:

QUESTION 285

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:

Explanation:

QUESTION 286

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:

Explanation:

QUESTION 287

Which of the following network security techniques can be easily circumvented by using a network sniffer?

- A. Disabling 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:

Explanation:

QUESTION 288

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:

Explanation:

QUESTION 289

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:

Explanation:

QUESTION 290

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:

Explanation:

QUESTION 291

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:

Explanation:

QUESTION 292

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:

Explanation:

QUESTION 293

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:

Explanation:

QUESTION 294

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:

Explanation:

QUESTION 295

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:

Explanation:

QUESTION 296

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:

Explanation:

QUESTION 297

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:

Explanation:

QUESTION 298

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:

Explanation:

QUESTION 299

Which of the following BEST describes the purpose of fuzzing?

- 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:

Explanation:

QUESTION 300

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:

Explanation:

QUESTION 301

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:

Explanation:

QUESTION 302

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:

Explanation:

QUESTION 303

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:

Explanation:

QUESTION 304

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:

Explanation:

QUESTION 305

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 306

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 307

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:

Explanation:

QUESTION 308

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:

Explanation:

QUESTION 309

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:

Explanation:

QUESTION 310

A security administrator is encrypting all smartphones 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:

Explanation:

QUESTION 311

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:

Explanation:

QUESTION 312

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 313

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 314

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 315

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:

Explanation:

QUESTION 316

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:

Explanation:

QUESTION 317

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 318

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

- A. $MTTR = (\text{time of fail}) / (\text{time of restore})$
- B. $MTTR = (\text{time of fail}) \# (\text{time of restore})$
- C. $MTTR = (\text{time of restore}) \# (\text{time of fail})$
- D. $MTTR = (\text{time of restore}) \times (\text{time of fail})$

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 319

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 is functioning?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 320

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:

Explanation:

QUESTION 321

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:

Explanation:

QUESTION 322

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 323

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 324

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

- A. Kerberos
- B. TFTP
- C. SSH
- D. DNS

Correct Answer: B

Section: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 325

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:
Explanation:

QUESTION 326

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 327

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:
Explanation:

QUESTION 328

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:

Explanation:

QUESTION 329

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:

Explanation:

QUESTION 330

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:

Explanation:

QUESTION 331

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:

Explanation:

QUESTION 332

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:

Explanation:

QUESTION 333

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 334

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:

Explanation:

QUESTION 335

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 336

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 337

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:

Explanation:

QUESTION 338

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:

Explanation:

QUESTION 339

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 340

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

- A. Impersonation
- B. Bluejacking
- C. War driving
- D. Bluesnarfing

Correct Answer: B

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 341

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:

Explanation:

QUESTION 342

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 343

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 344

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. Sniffers
- D. NIPS

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 345

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:

Explanation:

QUESTION 346

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:

Explanation:

QUESTION 347

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 348

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 349

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:

Explanation:

QUESTION 350

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 351

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:

Explanation:

QUESTION 352

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 353

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:
Explanation:

QUESTION 354

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:
Explanation:

QUESTION 355

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 356

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 357

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 358

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:

Explanation:

QUESTION 359

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

- A. USB encryptor
- B. Hardware write lock
- C. USB extension cable

D. Ext2 file system

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 360

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-Mas attack
- B. DDoS attack
- C. DNS poisoning
- D. DOS attack

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 361

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 phishing
- B. Spam
- C. Spim
- D. Spoofing

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 362

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:

Explanation:

QUESTION 363

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:

Explanation:

QUESTION 364

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:

Explanation:

QUESTION 365

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:

Explanation:

QUESTION 366

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. Fuzzing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 367

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:

Explanation:

QUESTION 368

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:

Explanation:

QUESTION 369

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:

Explanation:

QUESTION 370

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:

Explanation:

QUESTION 371

Which of the following is considered strong authentication?

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

Correct Answer: D

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 372

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 373

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:

Explanation:

QUESTION 374

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 375

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:

Explanation:

QUESTION 376

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:

Explanation:

QUESTION 377

Which of the following is another name for fuzzer 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:

Explanation:

QUESTION 378

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 379

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 baselining
- C. Virtualization
- D. Code review

Correct Answer: B

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 380

Which of the following software types can Sara, a security technician, use to protect against non-malicious but irritating malware?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 381

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:
Explanation:

QUESTION 382

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:
Explanation:

QUESTION 383

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: Pretest
Explanation

Explanation/Reference:
Explanation:

QUESTION 384

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:

Explanation:

QUESTION 385

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:

Explanation:

QUESTION 386

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:

Explanation:

QUESTION 387

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 388

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 389

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:

Explanation:

QUESTION 390

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 391

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 392

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 393

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:

Explanation:

QUESTION 394

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:

Explanation:

QUESTION 395

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:

Explanation:

QUESTION 396

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:

Explanation:

QUESTION 397

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:

Explanation:

QUESTION 398

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 399

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:

Explanation:

QUESTION 400

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:

Explanation:

QUESTION 401

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 subnetted.
- D. The switch needs to be virtualized and a new DMZ needs to be created.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 402

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:

Explanation:

QUESTION 403

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:

Explanation:

QUESTION 404

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 405

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:

Explanation:

QUESTION 406

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 407

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:

Explanation:

QUESTION 408

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:

Explanation:

QUESTION 409

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:

Explanation:

QUESTION 410

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:

Explanation:

QUESTION 411

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. Spyware
- D. Ransomware

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 412

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 a non-routable network
- D. On a secure internal network

Correct Answer: B

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 413

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 414

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:

Explanation:

QUESTION 415

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 416

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 417

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 418

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:

Explanation:

QUESTION 419

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 420

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:

Explanation:

QUESTION 421

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:

Explanation:

QUESTION 422

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. BitLocker

Correct Answer: A

Section: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 423

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:

Explanation:

QUESTION 424

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:

Explanation:

QUESTION 425

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 426

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:

Explanation:

QUESTION 427

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 428

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:

Explanation:

QUESTION 429

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 430

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. Fuzzing
- C. XSS
- D. Error handling

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 431

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 432

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:

Explanation:

QUESTION 433

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:

Explanation:

QUESTION 434

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:

Explanation:

QUESTION 435

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 436

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 437

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 438

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:

Explanation:

QUESTION 439

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 440

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:

Explanation:

QUESTION 441

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 442

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:

Explanation:

QUESTION 443

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:

Explanation:

QUESTION 444

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:

Explanation:

QUESTION 445

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:

Explanation:

QUESTION 446

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: Pretest

Explanation

Explanation/Reference:

Explanation:

QUESTION 447

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: Pretest

Explanation

Explanation/Reference:



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