COMPTIA SY0-201 EXAM BUNDLE

Number: SY0-201
Passing Score: 764
Time Limit: 90 min
File Version: 34.7

http://www.gratisexam.com/

COMPTIA SY0-201 EXAM BUNDLE

Exam Name: Comptia CompTIA Security+(2008 Edition) Exam

Examsoon

QUESTION 1
Who is responsible for establishing access permissions to network resources in the DAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The system administrator and the owner of the resource.
D. The user requiring access to the resource.

Correct Answer: B
Section: (none)
Explanation

QUESTION 2
The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. The public key infrastructure is based on which encryption schemes?

A. Symmetric
B. Quantum
C. Asymmetric
D. Elliptical curve

Correct Answer: C
Section: (none)
Explanation

QUESTION 3
Why will a Faraday cage be used?

A. To find rogue access points
B. To allow wireless usage
C. To mitigate data emanation
D. To minimize weak encryption

Correct Answer: C
Section: (none)
Explanation

QUESTION 4
The hashing algorithm is created from a hash value, making it nearly impossible to derive the original input number. Which item can implement the strongest hashing algorithm?

A. NTLMv2
B. LANMAN
C. NTLM
D. VLAN

Correct Answer: A
Section: (none)

Explanation

QUESTION 5
For which reason are clocks used in Kerberos authentication?

A. Clocks are used to ensure proper connections.
B. Clocks are used to ensure that tickets expire correctly.
C. Clocks are used to generate the seed value for the encryptions keys.
D. Clocks are used to both benchmark and specify the optimal encryption algorithm.

Correct Answer: B
Section: (none)
Explanation

QUESTION 6
A travel reservation organization conducts the majority of its transactions via a public facing website. Any downtime to this website will lead to serious financial damage for this organization. One web server is connected to several distributed database servers. Which statement is correct about this scenario?

A. RAID
B. Warm site
C. Proxy server
D. Single point of failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following is a common type of attack on web servers?

A. Birthday
B. Buffer overflow
C. Spam
D. Brute force

Correct Answer: B
Section: (none)
Explanation

QUESTION 8
The employees at a company are using instant messaging on company networked computers. The MOST important security issue to address when using instant messaging is that instant messaging:

A. Communications are a drain on bandwidth
B. Communications are open and unprotected
C. Has no common protocol
D. Uses weak encryption

Correct Answer: B
Section: (none)
Explanation

QUESTION 9
Removable storage has been around almost as long as the computer itself. Which of the following is the GREATEST security risk regarding removable storage?

A. Availability of data
B. Integrity of data
C. Not enough space available
D. Confidentiality of data

Correct Answer: D
Section: (none)
Explanation

QUESTION 10
In which authentication model a ticket granting server is an important concept?

A. CHAP
B. PAP
C. Kerberos
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

QUESTION 11
Which of the following would be needed to ensure that a user who has received an email cannot claim that the email was not received?

A. Anti-aliasing
B. Data integrity
C. Asymmetric cryptography
D. Non-repudiation

Correct Answer: D
Section: (none)
Explanation

QUESTION 12
In a secure environment, which authentication mechanism will perform better?

A. RADIUS because it encrypts client-server passwords.
B. TACACS because it encrypts client-server negotiation dialogs.
C. TACACS because it is a remote access authentication service.
D. RADIUS because it is a remote access authentication service.

Correct Answer: B
Section: (none)
Explanation

QUESTION 13
Which of the following types of firewalls provides inspection at layer 7 of the OSI model?

A. Application-proxy
B. Network address translation (NAT)
C. Packet filters
D. Stateful inspection

Correct Answer: A
Section: (none)
Explanation

QUESTION 14
Giving each user or group of users only the access they need to do their job is an example of which of the following security principals?

A. Least privilege
B. Defense in depth
C. Separation of duties
D. Access control

Correct Answer: A
Section: (none)
Explanation

QUESTION 15
A company implements an SMTP server on their firewall. This implementation would violate which of the following security principles?

A. Keep the solution simple
B. Use a device as intended
C. Create an in-depth defense
D. Address internal threats

Correct Answer: B
Section: (none)
Explanation

QUESTION 16
A company is upgrading the network and needs to reduce the ability of users on the same floor and network segment to see each other's traffic. Which of the following network devices should be used?

A. Router
B. Hub
C. Switch
D. Firewall

Correct Answer: C
Section: (none)
Explanation

QUESTION 17
In computing, a Uniform Resource Locator (URL) is a type of Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it. When a user attempts to go to a website, he notices the URL has changed, which attack will MOST likely cause the problem?

A. ARP poisoning
B. DLL injection
C. DNS poisoning
D. DDoS attack

Correct Answer: C
Section: (none)
Explanation

QUESTION 18
What does the DAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

QUESTION 19
After analyzing vulnerability and applying a security patch, which non-intrusive action should be taken to verify that the vulnerability was truly removed?

A. Update the antivirus definition file.
B. Apply a security patch from the vendor.
C. Repeat the vulnerability scan.
D. Perform a penetration test.

Correct Answer: C

Section: (none)
Explanation

QUESTION 20
A companys security' specialist is securing a web server that is reachable from the Internet. The web server is located in the core internal corporate network. The network cannot be redesigned and the server cannot be moved. Which of the following should the security specialist implement to secure the web server? (Select TWO).

A. Router with an IDS module
B. Network-based IDS
C. Router with firewall rule set
D. Host-based IDS
E. Network-based firewal
F. Host-based firewall

Correct Answer: DF
Section: (none)
Explanation

QUESTION 21
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Which method can be used to perform denial of service (DoS) attacks?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 22
The CHAP (Challenge Handshake Authentication Protocol) sends a logon request from the client to the server, and the server sends a challenge back to the client. At which stage does the CHAP protocol perform the handshake process? Choose the best complete answer.

A. At the stage when the connection is established and at whichever time after the connection has been established.
B. At the stage when the connection is established and when the connection is disconnected.
C. At the stage when the connection is established.
D. At the stage when the connection is disconnected.

Correct Answer: A
Section: (none)
Explanation

QUESTION 23
A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into

computers by monitoring network traffic. Which NIDS configuration is solely based on specific network traffic?

A. Anomaly-based
B. Host-based
C. Behavior-based
D. Signature-based

Correct Answer: D
Section: (none)
Explanation

QUESTION 24
Which of the following are nonessential protocols and services?

A. Network News Transfer Protocol (NNTP)
B. TFTP (Trivial File Transfer Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B
Section: (none)
Explanation

QUESTION 25
You work as a network technician for your company. The company policy for availability needs full backups on Sunday and incremental backups each week night at 10 p.m. The file server crashes on Wednesday afternoon; how many types are required to restore the data on the file server for Thursday morning?

A. One
B. Two
C. Three
D. Four

Correct Answer: C
Section: (none)
Explanation

QUESTION 26
Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. Network News Transfer Protocol (NNTP)
B. SNMP (Simple Network Management Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B
Section: (none)
Explanation

QUESTION 27
Which is the correct order in which crucial equipment should draw power?

A. Backup generator, UPS battery, UPS line conditioner
B. Uninterruptible Power Supply (UPS) battery, UPS line conditioner, backup generator
C. Backup generator, UPS line conditioner, UPS battery
D. UPS line conditioner, UPS battery, and backup generator

Correct Answer: D
Section: (none)
Explanation

QUESTION 28
Most key fob based identification systems use which of the following types of authentication mechanisms? (Select TWO).

A. Kerberos
B. Biometrics
C. Username/password
D. Certificates
E. Token

Correct Answer: CE
Section: (none)
Explanation

QUESTION 29
Alexander works as a network administrator for an organization which has 33,000 users. Now, Alexander wants to store six months of Internet proxy logs on a dedicated logging server for analysis and content reporting. The reports are not time critical, but are required by upper management for legal obligations. When determining the requirements for the logging server, which of the following will not be applied?

A. Log storage and backup requirements.
B. Log details and level of verbose logging.
C. Performance baseline and audit trails.
D. Time stamping and integrity of the logs.

Correct Answer: C
Section: (none)
Explanation

QUESTION 30
Which item will MOST likely permit an attacker to make a switch function like a hub?

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

Correct Answer: A

Section: (none)
Explanation

QUESTION 31
Which of the following describes a server or application that is accepting more input than the server or application is expecting?

A. Denial of service (DoS)
B. Syntax error
C. Buffer overflow
D. Brute force

Correct Answer: C
Section: (none)
Explanation

QUESTION 32
The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "authentication"), and to provide protection against replays. Which of the following is correct about authentication headers (AH)?

A. The authentication information is a keyed hash based on all of the bytes in the packet.
B. The authentication information may be the same on different packets if the integrity remains in place.
C. The authentication information hash will increase by one if the bytes remain the same on transfer.
D. The authentication information hash will remain the same if the bytes change on transfer.

Correct Answer: A
Section: (none)
Explanation

QUESTION 33
Which of the following refers to the ability to be reasonably certain that data is not modified or tampered with?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 34
Which description is correct about the form used while transferring evidence?

A. Evidence log
B. Booking slip
C. Chain of custody

D. Affidavit

Correct Answer: C
Section: (none)
Explanation

QUESTION 35
Disguising oneself as a reputable hardware manufacturer's field technician who is picking up a server for repair would be described as:

A. A phishing attack
B. A Trojan horse
C. A man-in-the-middle attack
D. Social engineering

Correct Answer: D
Section: (none)
Explanation

QUESTION 36
A graphical user interface (GUI) is a type of user interface which allows people to interact with electronic devices such as computers; hand-held devices such as MP3 Players, Portable Media Players or Gaming devices; household appliances and office equipment. Which of the following will allow a technician to restrict a user accessing to the GUI?

A. Use of logical tokens
B. Group policy implementation
C. Password policy enforcement
D. Access control lists

Correct Answer: B
Section: (none)
Explanation

QUESTION 37
A security specialist has downloaded a free security software tool from a trusted industry site. The source has published the MD5 hash values for the executable program. The specialist performs a successful virus scan on the download but the MD5 hash is different. Which of the following steps should the specialist take?

A. Avoid executing the file and contact the source website administrator
B. Ignore the MD5 hash values because the values can change during IP fragmentation.
C. Re-run the anti-virus program to ensure that it contains no virus execute
D. Install the executable program because there was probably a mistake with the MD5 value.

Correct Answer: A
Section: (none)
Explanation

QUESTION 38
Which authentication method will prevent a replay attack from occurring?

A. RADIUS
B. L2TP
C. Kerberos
D. CHAP

Correct Answer: C
Section: (none)
Explanation

QUESTION 39
Which of the following identifies the layer of the OSI model where SSL provides encryption?

A. Application
B. Network
C. Session
D. Transport

Correct Answer: C
Section: (none)
Explanation

QUESTION 40
Which of the following refers to the ability to be reasonably certain that data is not disclosed to unintended persons?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 41
Which of the following can be used by a technician to detect staff members that are connecting to an unauthorized website?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 42
Which of the following would be the BEST reason to disable unnecessary services on a server?

A. Not starting a service will save system memory and reduce startup time.

B. If a service doesn't support the function of the server the service won't be missed.
C. Attack surface and opportunity for compromise are reduced
D. Services can be re-enabled if needed at a later time

Correct Answer: C
Section: (none)
Explanation

QUESTION 43
For the following items, which is an example of an attack that executes once a year on a certain date?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 44
Access controls based on security labels associated with each data item and each user are known as:

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 45
Which tool can help the technician to find all open ports on the network?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 46
A user is assigned access rights explicitly. This is a feature of which of the following access control models?

A. Discretionary Access Control (DAC)

B. Mandatory Access Control (MAC)
C. Rule Based Access Control (RBAC)
D. Role Based Access Control (RBAC)

Correct Answer: A
Section: (none)
Explanation

QUESTION 47
Which algorithms can best encrypt large amounts of data?

A. Asymmetric key algorithms
B. Symmetric key algorithms
C. ECC algorithms
D. Hashing algorithms

Correct Answer: B
Section: (none)
Explanation

QUESTION 48
Which of the following describes an attacker encouraging a person to perform an action in order to be successful?

A. Man-in-the-middle
B. Social engineering
C. Back door
D. Password guessing

Correct Answer: B
Section: (none)
Explanation

QUESTION 49
During which phase of identification and authentication does proofing occur?

A. Authentication
B. Testing
C. Verification
D. Identification

Correct Answer: D
Section: (none)
Explanation

QUESTION 50
A user has received an email from a mortgage company asking for personal information including bank account numbers. This would BEST be described as:

A. Spam
B. Phishing

C. Packet sniffing
D. A hoax

Correct Answer: B
Section: (none)
Explanation

QUESTION 51
Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database. Which description is correct when a hashing algorithm generates the same hash for two different messages?

A. A one-way hash occurred.
B. A hashing chain occurred.
C. A collision occurred.
D. A deviation occurred.

Correct Answer: C
Section: (none)
Explanation

QUESTION 52
Which item can reduce the attack surface of an operating system?

A. Installing HIDS
B. Patch management
C. Installing antivirus
D. Disabling unused services

Correct Answer: D
Section: (none)
Explanation

QUESTION 53
Which of the following connectivity is required for a web server that is hosting an SSL based web site?

A. Port 443 inbound
B. Port 443 outbound
C. Port 80 inbound
D. Port 80 outbound

Correct Answer: A
Section: (none)
Explanation

QUESTION 54
For the following items, which is a protocol analyzer?

A. Cain Abel

B. WireShark
C. Nessus
D. John the Ripper

Correct Answer: B
Section: (none)
Explanation

QUESTION 55
Malicious port scanning is a method of attack to determine which of the following?

A. Computer name
B. The fingerprint of the operating system
C. The physical cabling topology of a network
D. User IDs and passwords

Correct Answer: B
Section: (none)
Explanation

QUESTION 56
Which description is correct about a way to prevent buffer overflows?

A. Apply all security patches to workstations.
B. Monitor P2P program usage through content filters.
C. Apply security templates enterprise wide.
D. Apply group policy management techniques.

Correct Answer: A
Section: (none)
Explanation

QUESTION 57
Which of the following is used to determine equipment status and modify the configuration or settings of network devices?

A. SNMP
B. DHCP
C. SMTP
D. CHAP

Correct Answer: A
Section: (none)
Explanation

QUESTION 58
Which item will effectively allow for fast, highly secure encryption of a USB flash drive?

A. 3DES
B. SHA-1

C. MD5
D. AES256

Correct Answer: D
Section: (none)
Explanation

QUESTION 59
Which of the following describes the process by which a single user name and password can be entered to access multiple computer applications?

A. Single sign-on
B. Encryption protocol
C. Access control lists
D. Constrained user interfaces

Correct Answer: A
Section: (none)
Explanation

QUESTION 60
Network traffic is data in a network. Which tool can be used to review network traffic for clear text passwords?

A. Port scanner
B. Protocol analyzer
C. Firewall
D. Password cracker

Correct Answer: B
Section: (none)
Explanation

QUESTION 61
To preserve evidence for later use in court, which of the following needs to be documented?

A. Audit trail of systems usage
B. Disaster recovery plan
C. Chain of certificates
D. Chain of custody

Correct Answer: D
Section: (none)
Explanation

QUESTION 62
Which of the following describes a type of algorithm that cannot be reversed in order to decode the data?

A. Symmetric
B. One Way Function

C. Asymmetric
D. Pseudorandom Number Generator (PRNG)

Correct Answer: B
Section: (none)
Explanation

QUESTION 63
What are best practices while installing and securing a new system for a home user? (Select THREE).

A. Use a strong firewall.
B. Install remote control software.
C. Apply all system patches.
D. Apply all service packs.

Correct Answer: ACD
Section: (none)
Explanation

QUESTION 64
Which of the following is a major reason that social engineering attacks succeed?

A. Strong passwords are not required
B. Lack of security awareness
C. Multiple logins are allowed
D. Audit logs are not monitored frequently

Correct Answer: B
Section: (none)
Explanation

QUESTION 65
Which security action should be finished before access is given to the network?

A. Identification and authorization
B. Identification and authentication
C. Authentication and authorization
D. Authentication and password

Correct Answer: B
Section: (none)
Explanation

QUESTION 66
Which of the following types of backups requires that files and software that have been changed since the last full backup be copied to storage media?

A. Incremental
B. Differential
C. Full

D. Delta

Correct Answer: B
Section: (none)
Explanation

QUESTION 67
Which port must be open to allow a user to login remotely onto a workstation?

A. 53
B. 636
C. 3389
D. 8080

Correct Answer: C
Section: (none)
Explanation

QUESTION 68
The authentication process where the user can access several resources without the need for multiple credentials is known as:

A. Discretionary Access Control (DAC).
B. Need to know
C. Decentralized management
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

QUESTION 69
Which item best describes an instance where a biometric system identifies legitimate users as being unauthorized?

A. False acceptance
B. False positive
C. False rejection
D. False negative

Correct Answer: C
Section: (none)
Explanation

QUESTION 70
The purpose of the SSID in a wireless network is to:

A. Define the encryption protocols used.
B. Secure the WAP
C. Identify the network
D. Protect the client

Correct Answer: C
Section: (none)
Explanation

QUESTION 71
Which of the following is the best description about the method of controlling how and when users can connect in from home?

A. Remote access policy
B. Remote authentication
C. Terminal access control
D. Virtual Private Networking (VPN)

Correct Answer: A
Section: (none)
Explanation

QUESTION 72
Which of the following would be the MOST common method for attackers to spoof email?

A. Web proxy
B. Man in the middle attacks
C. Trojan horse programs
D. Open relays

Correct Answer: D
Section: (none)
Explanation

QUESTION 73
CRL is short for Certificate Revocation List. Which types of keys are included in a CRL?

A. Both public and private keys
B. Public keys
C. Steganographic keys
D. Private keys

Correct Answer: A
Section: (none)
Explanation

QUESTION 74
The implicit deny will block anything you didn't specifically allow but you may have allowed stuff that you don't need. A technician is reviewing the system logs for a firewall and is told that there is an implicit deny within the ACL. Which is an example of an implicit deny?

A. An implicit deny statement denies all traffic from one network to another.
B. Each item is denied by default because of the implicit deny.
C. Items which are not specifically given access are denied by default.
D. An ACL is a way to secure traffic from one network to another.

Correct Answer: C
Section: (none)
Explanation

QUESTION 75
Which of the following is often misused by spyware to collect and report a user's activities?

A. Persistent cookie
B. Web bug
C. Tracking cookie
D. Session cookie

Correct Answer: C
Section: (none)
Explanation

QUESTION 76
Which of the following is not identified within the penetration testing scope of work?

A. A complete list of all network vulnerabilities.
B. Handling of information collected by the penetration testing team.
C. IP addresses of machines from which penetration testing will be executed.
D. A list of acceptable testing techniques and tools to be utilized.

Correct Answer: A
Section: (none)
Explanation

QUESTION 77
Choose the figure which represents the number of ports in the TCP/IP (Transmission Control Protocol/Internet Protocol) which are vulnerable to being scanned, attacked, and exploited.

A. 32 ports
B. 1,024 ports
C. 65,535 ports
D. 16,777,216 ports

Correct Answer: C
Section: (none)
Explanation

QUESTION 78
Tom is a network technician of his company. Now, he is making a decision between implementing a HIDS on the database server and implementing a NIDS. Why NIDS may be better to implement? (Select TWO).

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

Correct Answer: BC
Section: (none)
Explanation

QUESTION 79
Which of the following would be considered a detrimental effect of a virus hoax? (Select TWO).

A. The email server capacity is consumed by message traffic.
B. Technical support resources are consumed by increased user calls.
C. Users are tricked into changing the system configuration.
D. Users are at risk for identity theft.

Correct Answer: BC
Section: (none)
Explanation

QUESTION 80
Which types of keys will be used if a server and workstation communicate via SSL? (Select TWO).

A. Public key
B. Recovery key
C. Session key
D. Keylogger

Correct Answer: AC
Section: (none)
Explanation

QUESTION 81
To keep an 802.11x network from being automatically discovered, a user should:

A. Turn off the SSID broadcast.
B. Leave the SSID default.
C. Change the SSID name.
D. Activate the SSID password

Correct Answer: A
Section: (none)
Explanation

QUESTION 82
Which security policy will be most likely used while attempting to mitigate the risks involved with allowing a user to access company email via their cell phone?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 83
Which of the following BEST describes the baseline process of securing devices on a network infrastructure?

A. Enumerating
B. Hardening
C. Active prevention
D. Passive detection

Correct Answer: B
Section: (none)
Explanation

QUESTION 84
Secret Key encryption is also known as:

A. Symmetrical
B. Replay
C. One way function.
D. Asymmetrical

Correct Answer: A
Section: (none)
Explanation

QUESTION 85
In computing, virtualization is a broad term that refers to the abstraction of computer resources. Which is a security reason to implement virtualization throughout the network infrastructure?

A. To implement additional network services at a lower cost
B. To analyze the various network traffic with protocol analyzers
C. To isolate the various network services and roles
D. To centralize the patch management of network servers

Correct Answer: C
Section: (none)
Explanation

QUESTION 86
Which of the following types of removable media is write-once and appropriate for archiving security logs?

A. Tape
B. CD-R
C. Hard disk
D. USB drive

Correct Answer: B
Section: (none)
Explanation

QUESTION 87
After installing new software on a machine, what needs to be updated to the baseline?

A. Honeypot
B. Signature-based NIPS
C. Signature-based NIDS
D. Behavior-based HIDS

Correct Answer: D
Section: (none)
Explanation

QUESTION 88
Which of the following could cause communication errors with an IPSec VPN tunnel because of changes made to the IP header?

A. SOCKS
B. NAT
C. DNS
D. Private addressing

Correct Answer: B
Section: (none)
Explanation

QUESTION 89
A PC is rejecting push updates from the server; all other PCs on the network are accepting the updates successfully. What should be examined first?

A. Password expiration
B. Local firewall
C. Anti-spyware
D. Pop-up blocker

Correct Answer: B
Section: (none)
Explanation

QUESTION 90
A company wants to connect the network to a manufacturer's network to be able to order parts. Which of the following types of networks should the company implement to provide the connection while limiting the services allowed over the connection?

A. Scatternet
B. Extranet
C. VPN
D. Intranet

Correct Answer: B
Section: (none)
Explanation

QUESTION 91
Malware, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. A network technician suspects that a piece of malware is consuming too many CPU cycles and slowing down a system. Which item can help determine the amount of CPU cycles being consumed?

A. Install malware scanning software.
B. Run performance monitor to evaluate the CPU usage.
C. Use a protocol analyzer to find the cause of the traffic.
D. Install HIDS to determine the CPU usage.

Correct Answer: B
Section: (none)
Explanation

QUESTION 92
Which of the following ports are typically used by email clients? (Select TWO)

A. 3389
B. 194
C. 143
D. 110
E. 49
F. 23

Correct Answer: CD
Section: (none)
Explanation

QUESTION 93
In order to allow for more oversight of past transactions, a company decides to exchange positions of the purchasing agent and the accounts receivable agent. Which is an example of this?

A. Separation of duties
B. Least privilege
C. Implicit deny
D. Job rotation

Correct Answer: D
Section: (none)
Explanation

QUESTION 94
Fiber optic cable is considered safer than CAT5 because fiber optic cable: (Select TWO).

A. Is not susceptible to interference.
B. Is hard to tap in to.
C. Is made of glass rather than copper.
D. Can be run for a longer distance
E. Is more difficult to install

Correct Answer: AB
Section: (none)
Explanation

QUESTION 95
Why do security researchers often use virtual machines?

A. To offer an environment where new network applications can be tested
B. To offer a secure virtual environment to conduct online deployments
C. To offer a virtual collaboration environment to discuss security research
D. To offer an environment where malware can be executed with minimal risk to equipment and software

Correct Answer: D
Section: (none)
Explanation

QUESTION 96
Virtualized applications, such as virtualized browsers, can protect the underlying operating system from which of the following?

A. Malware installation from suspects Internet sites
B. DDoS attacks against the underlying OS
C. Man-in-the-middle attacks
D. Phishing and spam attacks

Correct Answer: A
Section: (none)
Explanation

QUESTION 97
How to make sure that when an employee leaves the company permanently, the company will have access to their private keys?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 98
A DNS (Domain Name Service) server uses a specific port number. Choose this port number

from the options.

A. Port 32
B. Port 1,024
C. Port 65,535
D. Port 16,777,216

Correct Answer: B
Section: (none)
Explanation

QUESTION 99
An outside auditor has been contracted to determine whether weak passwords are being used on the network. In order to achieve this goal, the auditor is running a password cracker against the master password file. Which of the following is an example of this?

A. Vulnerability assessment
B. Malware scan
C. Baselining
D. Fingerprinting

Correct Answer: A
Section: (none)
Explanation

QUESTION 100
Which of the following access attacks would involve looking through your files in the hopes of finding something interesting?

A. Interception
B. Snooping
C. Eavesdropping
D. None of the above

Correct Answer: B
Section: (none)
Explanation

QUESTION 101
Identify the service provided by message authentication code (MAC) hash:

A. Data recovery.
B. Fault tolerance.
C. Key recovery.
D. Integrity

Correct Answer: D
Section: (none)
Explanation

QUESTION 102

A company wants to implement a VLAN. Senior management believes that a VLAN will be secure because authentication is accomplished by MAC addressing and that dynamic trunking protocol (DTP) will facilitate network efficiency. Which of the following issues should be discussed with senior management before VLAN implementation?

A. MAC addresses can be spoofed and DTP allows rogue network devices to configure ports
B. MAC addresses can be spoofed and DTP allows only authenticated users.
C. MAC addresses are a secure authentication mechanism and DTP allows rogue network devices to configure ports.
D. MAC addresses are a secure authentication mechanism and DTP allows only authenticated users.

Correct Answer: A
Section: (none)
Explanation

QUESTION 103
John works as a network administrator for his company. On the monthly firewall log, he discovers that many internal PCs are sending packets on a routine basis to a single external PC. Which statement correctly describes what is happening?

A. The remote PC has a zombie slave application running and the local PCs have a zombie master application running.
B. The remote PC has a zombie master application running and the local PCs have a zombie slave application running.
C. The remote PC has a spam slave application running and the local PCs have a spam master application running.
D. The remote PC has a spam master application running and the local PCs have a spam slave application running.

Correct Answer: B
Section: (none)
Explanation

QUESTION 104
Pretty Good Privacy (PGP) uses a PKI Trust Model where no certificate authority (CA) is subordinate to another. The model with no single trusted root is known as:

A. Peer-to-peer
B. Downlevel
C. Hierarchical
D. Hybrid

Correct Answer: A
Section: (none)
Explanation

QUESTION 105
Which key can be used by a user to log into their network with a smart card?

A. Public key
B. Cipher key

C. Shared key
D. Private key

Correct Answer: D
Section: (none)
Explanation

QUESTION 106
Which of the following would be an effective way to ensure that a compromised PKI key can not access a system?

A. Reconfigure the key
B. Revoke the key
C. Delete the key
D. Renew the key

Correct Answer: B
Section: (none)
Explanation

QUESTION 107
What does the MAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above

Correct Answer: A
Section: (none)
Explanation

QUESTION 108
Which description is true about the process of securely removing information from media (e.g. hard drive) for future use?

A. Deleting
B. Reformatting
C. Sanitization
D. Destruction

Correct Answer: C
Section: (none)
Explanation

QUESTION 109
Which of the following provides the MOST secure form of encryption?

A. 3DES
B. Diffie-Hellman

C. DES
D. AES

Correct Answer: D
Section: (none)
Explanation

QUESTION 110
Users on a network report that they are receiving unsolicited emails from the same email address. Which action should be performed to prevent this from occurring?

A. Install an ACL on the firewall to block traffic from the sender and filter the IP address.
B. Configure a rule in each users router and restart the router.
C. Install an anti-spam filter on the domain mail servers and filter the email address.
D. Configure rules on the users host and restart the host.

Correct Answer: C
Section: (none)
Explanation

QUESTION 111
Which of the following describes the validation of a message's origin?

A. Integrity
B. Confidentiality
C. Non-repudiation
D. Asymmetric encryption

Correct Answer: C
Section: (none)
Explanation

QUESTION 112
Users are using thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which mitigation technique would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Apply the concept of least privilege to USB devices.
C. Disable USB within the workstations BIOS.
D. Run spyware detection against all workstations.

Correct Answer: AC
Section: (none)
Explanation

QUESTION 113
Using software on an individual computer to generate a key pair is an example of which of the following approaches to PKI architecture?

A. Decentralized

B. Centralized
C. Hub and spoke
D. Distributed key

Correct Answer: A
Section: (none)
Explanation

QUESTION 114
Which description is true about how to accomplish steganography in graphic files?

A. Replacing the most significant bit of each byte
B. Replacing the most significant byte of each bit
C. Replacing the least significant byte of each bit
D. Replacing the least significant bit of each byte

Correct Answer: D
Section: (none)
Explanation

QUESTION 115
Which of the following types of encryption would be BEST to use for a large amount of data?

A. Asymmetric
B. Symmetric
C. ROT13
D. Hash

Correct Answer: B
Section: (none)
Explanation

QUESTION 116
Which one of the following options is a vulnerability assessment tool?

A. AirSnort
B. John the Ripper
C. Cain Abel
D. Nessus

Correct Answer: D
Section: (none)
Explanation

QUESTION 117
Malicious software that travels across computer networks without user assistance is an example of a:

A. Worm
B. Virus

C. Logic bomb
D. Trojan hors

Correct Answer: A
Section: (none)
Explanation

QUESTION 118
For the following items, which one is a collection of servers setup to attract hackers?

A. Honeypot
B. VLAN
C. Honeynet
D. DMZ

Correct Answer: C
Section: (none)
Explanation

QUESTION 119
You work as a network administrator for your company. Your company has just detected a malware incident. Which will be your first response?

A. Removal
B. Containment
C. Recovery
D. Monitor

Correct Answer: B
Section: (none)
Explanation

QUESTION 120
When setting password rules, which of the following would lower the level of security of a network?

A. Passwords must be greater than six characters and contain at least one non-alpha.
B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
C. Complex passwords that users can not remotely change are randomly generated by the administrator and given to users
D. After a set number of failed attempts the server will lock out any user account forcing the user to call the administrator to re-enable the account.

Correct Answer: C
Section: (none)
Explanation

QUESTION 121
You are a network technician of your company. You have just detected an intrusion on your company??s network from the Internet. What should be checked FIRST?

A. The firewall logs
B. The performance logs
C. The DNS logs
D. The access logs

Correct Answer: A
Section: (none)
Explanation

QUESTION 122
A person pretends to be a telecommunications repair technician, enters a building stating that there is a networking trouble work order and requests that a security guard unlock the wiring closet. The person connects a packet sniffer to the network switch in the wiring closet and hides the sniffer behind the switch against a wall. This is an example of:

A. A vulnerability scan
B. Social engineering
C. A man in the middle attack
D. A penetration test

Correct Answer: B
Section: (none)
Explanation

QUESTION 123
Which method could identify when unauthorized access has occurred?

A. Implement session termination mechanism.
B. Implement previous logon notification.
C. Implement session lock mechanism.
D. Implement two-factor authentication.

Correct Answer: B
Section: (none)
Explanation

QUESTION 124
Which of the following definitions would be correct regarding Eavesdropping?

A. Placing a computer system between the sender and receiver to capture information.
B. Someone looking through your files.
C. Listening or overhearing parts of a conversation
D. Involve someone who routinely monitors network traffic.

Correct Answer: C
Section: (none)
Explanation

QUESTION 125
Which practice is the best to secure log files?

A. Copy or save the logs to a remote log server.
B. Change security settings to avoid corruption.
C. Log all failed and successful login attempts.
D. Deny administrators all access to log files to prevent write failures.

Correct Answer: A
Section: (none)
Explanation

QUESTION 126
Which of the following definitions would be correct regarding Active Inception?

A. Someone looking through your files
B. Involve someone who routinely monitors network traffic
C. Listening or overhearing parts of a conversation
D. Placing a computer system between the sender and receiver to capture information.

Correct Answer: D
Section: (none)
Explanation

QUESTION 127
How to test the integrity of a company's backup data?

A. By reviewing the written procedures
B. By conducting another backup
C. By restoring part of the backup
D. By using software to recover deleted files

Correct Answer: C
Section: (none)
Explanation

QUESTION 128
Nmap has been run against a server and more open ports than expected have been discovered.
Which of the following would be the FIRST step to take?

A. All ports should be closed and observed to see whether a process tries to reopen the port.
B. Nmap should be run again and observed to see whether different results are obtained.
C. All ports should be left open and traffic monitored for malicious activity
D. The process using the ports should be examined.

Correct Answer: D
Section: (none)
Explanation

QUESTION 129
Which of the following statements regarding the MAC access control models is TRUE?

A. The Mandatory Access Control (MAC) model is a dynamic model.

B. In the Mandatory Access Control (MAC) the owner of a resource establishes access privileges to that resource.
C. In the Mandatory Access Control (MAC) users cannot share resources dynamically.
D. The Mandatory Access Control (MAC) model is not restrictive.

Correct Answer: C
Section: (none)
Explanation

QUESTION 130
Which statement best describes a static NAT?

A. A static NAT uses a many to many mapping.
B. A static NAT uses a one to many mapping.
C. A static NAT uses a many to one mapping.
D. A static NAT uses a one to one mapping.

Correct Answer: D
Section: (none)
Explanation

QUESTION 131
Which of the following would be MOST desirable when attacking encrypted data?

A. Sniffed traffic
B. Block cipher
C. Weak key
D. Algorithm used

Correct Answer: C
Section: (none)
Explanation

QUESTION 132
Which scanner can find a rootkit?

A. Email scanner
B. Malware scanner
C. Anti-spam scanner
D. Adware scanner

Correct Answer: B
Section: (none)
Explanation

QUESTION 133
Social engineering attacks would be MOST effective in which of the following environments? (Select TWO).

A. A locked, windowless building
B. A military facility with computer equipment containing biometrics.

C. A public building that has shared office space.
D. A company with a dedicated information technology (IT) security staff.
E. A company with a help desk whose personnel have minimal training.

Correct Answer: CE
Section: (none)
Explanation

QUESTION 134
What is steganography primarily used for?

A. Data integrity
B. Message digest
C. Hide information
D. Encrypt information

Correct Answer: C
Section: (none)
Explanation

QUESTION 135
Which of the following is the MOST effective way for an administrator to determine what security holes reside on a network?

A. Perform a vulnerability assessment
B. Run a port scan
C. Run a sniffer
D. Install and monitor an IDS

Correct Answer: A
Section: (none)
Explanation

QUESTION 136
For the following sites, which one has the means (e.g. equipment, software, and communications) to facilitate a full recovery within minutes?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 137
A company has instituted a VPN to allow remote users to connect to the office. As time progresses multiple security associations are created with each association being more secure. Which of the following should be implemented to automate the selection of the BEST security association for each user?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 138
Which item is not a logical access control method?

A. Biometrics
B. Group policy.
C. ACL
D. Software token.

Correct Answer: A
Section: (none)
Explanation

QUESTION 139
The concept that a web script is run in its own environment and cannot interfere with any other process is known as a:

A. Honey pot
B. VLAN
C. Quarantine
D. Sandbox

Correct Answer: D
Section: (none)
Explanation

QUESTION 140
Which description is correct about an application or string of code that could not automatically spread from one system to another but is designed to spread from file to file?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 141
Which description is true about the external security testing?

A. Conducted from outside the perimeter switch but inside the border router
B. Conducted from outside the perimeter switch but inside the firewall
C. Conducted from outside the organizations security perimeter
D. Conducted from outside the building that hosts the organizations servers

Correct Answer: C
Section: (none)
Explanation

QUESTION 142
A small manufacturing company wants to deploy secure wireless on their network. Which of the following wireless security protocols could be used? (Select TWO).

A. WEP
B. IPX
C. WPA
D. WAN

Correct Answer: AC
Section: (none)
Explanation

QUESTION 143
What should be established immediately upon evidence seizure?

A. Forensic analysis
B. Start the incident respond plan
C. Chain of custody
D. Damage and loss control

Correct Answer: C
Section: (none)
Explanation

QUESTION 144
Which of the following uses private key / public key technology to secure web sites?

A. SSL
B. TCP
C. Media Access Control (MAC)
D. Access Control List (ACL)

Correct Answer: A
Section: (none)
Explanation

QUESTION 145
Which one of the following options will permit an attacker to hide the presence of malicious code through altering the systems process and registry entries?

A. Trojan

B. Logic bomb
C. Worm
D. Rootkit

Correct Answer: D
Section: (none)
Explanation

QUESTION 146
Which of the following is the MOST significant flaw in Pretty Good Privacy (PGP) authentication?

A. Private keys can be compromised.
B. A user must trust the public key that is received
C. It is subject to a man-in-the-middle attack
D. Weak encryption can be easily broken

Correct Answer: B
Section: (none)
Explanation

QUESTION 147
Patch management must be combined with full-featured systems management to be effective. Determining which patches are needed, applying the patches and which of the following are three generally accepted activities of patch management?

A. Backing up the patch file executables to a network share
B. Updating the firewall configuration to include the patches
C. Auditing for the successful application of the patches
D. Running a NIDS report to list the remaining vulnerabilities

Correct Answer: C
Section: (none)
Explanation

QUESTION 148
The MOST common exploits of Internet-exposed network services are due to:

A. Illicit servers
B. Trojan horse programs
C. Active content (e.g. Java Applets)
D. Buffer overflows

Correct Answer: D
Section: (none)
Explanation

QUESTION 149
Which option is correct about a hash algorithms ability to avoid the same output from two guessed inputs?

A. Collision strength

B. Collision resistance
C. Collision strength
D. Collision metric

Correct Answer: B
Section: (none)
Explanation

QUESTION 150
Which of the following would be an example of a hardware device where keys can be stored? (Select TWO).

A. PCI card
B. Smart card
C. PCMCIA card
D. Network interface card (NIC)

Correct Answer: BC
Section: (none)
Explanation

QUESTION 151
Which of the following are types of certificate-based authentication? (Select TWO)

A. Many-to-one mapping
B. One-to-one mapping
C. One-to-many mapping
D. Many-to-many mapping

Correct Answer: AB
Section: (none)
Explanation

QUESTION 152
Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Which encryption is the strongest by use of mathematical evaluation techniques?

A. 3DES
B. ROT13
C. AES
D. DES

Correct Answer: C
Section: (none)
Explanation

QUESTION 153
The Diffie-Hellman encryption algorithm relies on which of the following?

A. Tunneling

B. Digital signatures
C. Key exchange
D. Passwords

Correct Answer: C
Section: (none)
Explanation

QUESTION 154
Which technology is able to isolate a host OS from some types of security threats?

A. Kiting
B. Virtualization
C. Cloning
D. Intrusion detection

Correct Answer: B
Section: (none)
Explanation

QUESTION 155
Non-repudiation is enforced by which of the following?

A. Secret keys
B. Digital signatures
C. PKI
D. Cipher block chaining

Correct Answer: B
Section: (none)
Explanation

QUESTION 156
Your company has already implemented two-factor authentication and wants to install a third authentication factor. If the existing authentication system uses strong passwords and PKI tokens, which item would provide a third factor?

A. Six digit PINs
B. Pass phrases
C. Fingerprint scanner
D. Elliptic curve

Correct Answer: C
Section: (none)
Explanation

QUESTION 157
Which of the following would be the MOST effective backup site for disaster recovery?

A. Cold site
B. Warm site

C. Hot site
D. Reciprocal agreement

Correct Answer: C
Section: (none)
Explanation

QUESTION 158
Which one of the following options will create a security buffer zone between two rooms?

A. Mantrap
B. Anti-pass back
C. DMZ
D. Turnstile

Correct Answer: A
Section: (none)
Explanation

QUESTION 159
Which of the following describes backing up files and software that have changed since the last full or incremental backup?

A. Full backup
B. Differential backup
C. Incremental backup
D. Delta backup

Correct Answer: C
Section: (none)
Explanation

QUESTION 160
Which is the primary objective to implement performance monitoring applications on network systems from a security standpoint?

A. To detect host intrusions from external networks
B. To detect network intrusions from external attackers
C. To detect integrity degradations to network attached storage
D. To detect availability degradations caused by attackers

Correct Answer: D
Section: (none)
Explanation

QUESTION 161
Human resource department personnel should be trained about security policy:

A. Guidelines and enforcement.
B. Maintenance.
C. Monitoring and administration

D. Implementation

Correct Answer: A
Section: (none)
Explanation

QUESTION 162
In computer security, an access control list (ACL) is a list of permissions attached to an object. Which log will reveal activities about ACL?

A. Performance
B. Mobile device
C. Firewall
D. Transaction

Correct Answer: C
Section: (none)
Explanation

QUESTION 163
Which of the following can affect heaps and stacks?

A. SQL injection
B. Cross-site scripting
C. Buffer overflows
D. Rootkits

Correct Answer: C
Section: (none)
Explanation

QUESTION 164
An enclosure that prevents radio frequency signals from emanating out of a controlled environment is BEST described as which of the following?

A. Faraday cage
B. Mantrap
C. Grounded wiring frame
D. TEMPEST

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Which of the following is not a step in the incident response?

A. Recovery.
B. Repudiation
C. Containment
D. Eradication

Correct Answer: B
Section: (none)
Explanation

QUESTION 166
In a classified environment, a clearance into a Top Secret compartment only allows access to certain information within that compartment. This is known as:

A. Dual control.
B. Need to know.
C. Separation of duties
D. Acceptable use.

Correct Answer: B
Section: (none)
Explanation

QUESTION 167
On the basis of certain ports, which of the following will allow wireless access to network resources?

A. 802.11a
B. 802.11n
C. 802.1x
D. 802.11g

Correct Answer: C
Section: (none)
Explanation

QUESTION 168
An organization has a hierarchical-based concept of privilege management with administrators having full access, human resources personnel having slightly less access and managers having access to their own department files only. This is BEST described as:

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

Correct Answer: D

Section: (none)
Explanation

QUESTION 169
Identify the item that can determine which flags are set in a TCP/IP handshake?

A. Network mapper
B. FIN/RST
C. Protocol analyzer
D. SYN/ACK

Correct Answer: C
Section: (none)
Explanation

QUESTION 170
A representative from the human resources department informs a security specialist that an employee has been terminated. Which of the following would be the BEST action to take?

A. Disable the employee's user accounts and keep the data for a specified period of time.
B. Disable the employee's user accounts and delete all data.
C. Contact the employee's supervisor regarding disposition of user accounts
D. Change the employee's user password and keep the data for a specified period.

Correct Answer: A
Section: (none)
Explanation

QUESTION 171
Which one of the following processes is best to remove PII data from a disk drive before reuse?

A. Reformatting
B. Sanitization
C. Degaussing
D. Destruction

Correct Answer: B
Section: (none)
Explanation

QUESTION 172
One of the below options are correct regarding the DDoS (Distributed Denial of Service) attack?

A. Listening or overhearing parts of a conversation
B. Placing a computer system between the sender and receiver to capture information
C. Use of multiple computers to attack a single organization
D. Prevention access to resources by users authorized to use those resources

Correct Answer: C
Section: (none)
Explanation

QUESTION 173
The ability to logon to multiple systems with the same credentials is typically known as:

A. Decentralized management
B. Single sign-on
C. Role Based Access Control (RBAC)
D. Centralized management

Correct Answer: B
Section: (none)
Explanation

QUESTION 174
Why malware that uses virtualization techniques is difficult to detect?

A. The malware may be implementing a proxy server for command and control.
B. A portion of the malware may have been removed by the IDS.
C. The malware may be using a Trojan to infect the system.
D. The malware may be running at a more privileged level than the antivirus software.

Correct Answer: D
Section: (none)
Explanation

QUESTION 175
An SMTP server is the source of email spam in an organization. Which of the following is MOST likely the cause?

A. The administrator account was not secured.
B. X.400 connectors have not been password protected.
C. Remote access to the email application's install directory has not been removed.
D. Anonymous relays have not been disabled.

Correct Answer: D
Section: (none)
Explanation

QUESTION 176
A graphical user interface (GUI) is a type of user interface which allows people to interact with electronic devices such as computers; hand-held devices such as MP3 Players, Portable Media Players or Gaming devices; household appliances and office equipment. Which of the following will permit a technician to restrict a users?? Access to the GUI?

A. Use of logical tokens
B. Group policy implementation
C. Password policy enforcement
D. Access control lists

Correct Answer: B
Section: (none)

Explanation

QUESTION 177
The first step in creating a security baseline would be:

A. Identifying the use case.
B. Installing software patches.
C. Vulnerability testing
D. Creating a security policy

Correct Answer: D
Section: (none)
Explanation

QUESTION 178
Which key is generally applied FIRST to a message digest to provide non-repudiation by use of asymmetric cryptography?

A. Private key of the receiver
B. Private key of the sender
C. Public key of the sender
D. Public key of the receiver

Correct Answer: B
Section: (none)
Explanation

QUESTION 179
Default passwords in hardware and software should be changed:

A. If a threat becomes known.
B. Once each month
C. When the hardware or software is turned on.
D. When the vendor requires it

Correct Answer: C
Section: (none)
Explanation

QUESTION 180
An organization needs to monitor all network traffic as it traverses their network. Which item should be used by the technician?

A. Honeypot
B. Protocol analyzer
C. HIDS
D. Content filter

Correct Answer: B
Section: (none)
Explanation

QUESTION 181
Which of the following types of programs autonomously replicates itself across networks?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 182
An accountant has logged onto the company's outside banking website. An administrator uses a TCP/IP monitoring tool to discover that the accountant was actually using a spoofed banking website. What most likely cause this attack? (Select TWO).

A. Altered hosts file
B. Bluesnarfing
C. Network mapper
D. DNS poisoning

Correct Answer: AD
Section: (none)
Explanation

QUESTION 183
Which of the following is employed to allow distrusted hosts to connect to services inside a network without allowing the hosts direct access to the internal networks?

A. VLAN
B. Extranet
C. Demilitarized zone (DMZ)
D. Intranet

Correct Answer: C
Section: (none)
Explanation

QUESTION 184
For the following options, which is an area of the network infrastructure that allows a technician to put public facing systems into it without compromising the entire infrastructure?

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

Correct Answer: D
Section: (none)

Explanation

QUESTION 185
You work as a network administrator for your company. Your company requires you to improve the physical security of a data center located inside the office building. The data center already maintains a physical access log and has a video surveillance system. Which additional control can be performed?

A. ACL
B. Defense-in-depth
C. Logical token
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

QUESTION 186
Which of the following BEST describes an attempt to transfer DNS zone data?

A. Evasion
B. Fraggle
C. Teardrop
D. Reconnaissance

Correct Answer: D
Section: (none)
Explanation

QUESTION 187
Which method is the LEAST intrusive to check the environment for known software flaws?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 188
A honeypot is used to:

A. Provide an unauthorized user with a place to safely work.
B. Give an unauthorized user time to complete an attack.
C. Trap attackers in a false network.
D. Allow administrators a chance to observe an attack.

Correct Answer: D
Section: (none)

Explanation

QUESTION 189
Which item can easily create an unencrypted tunnel between two devices?

A. PPTP
B. AES
C. L2TP
D. HTTPS

Correct Answer: C
Section: (none)
Explanation

QUESTION 190
Which of the following are components of host hardening? (Select TWO).

A. Removing a user's access to the user's data.
B. Adding users to the administrator group.
C. Disabling unnecessary services.
D. Configuring the Start menu and Desktop
E. Applying patches

Correct Answer: CE
Section: (none)
Explanation

QUESTION 191
In order to encrypt credit card data, which will be the most secure algorithm with the least CPU utilization?

A. 3DES
B. AES
C. SHA-1
D. MD5

Correct Answer: B
Section: (none)
Explanation

QUESTION 192
Which of the following statements regarding authentication protocols is FALSE?

A. PAP is insecure because usernames and passwords are sent over the network in clear text.
B. CHAP is more secure than PAP because it encrypts usernames and passwords before they are sent over the network.
C. RADIUS is a client/server-based system that provides authentication, authorization, and accounting services for remote dial-up access.
D. MS-CHAP version 1 is capable of mutual authentication of both the client and the server.

Correct Answer: D

Section: (none)
Explanation

QUESTION 193
Which solution can be used by a user to implement very tight security controls for technicians that seek to enter the users' datacenter?

A. Combination locks and key locks
B. Smartcard and proximity readers
C. Magnetic lock and pin
D. Biometric reader and smartcard

Correct Answer: D
Section: (none)
Explanation

QUESTION 194
Which of the following is a protocol analyzer?

A. John the Ripper
B. WireShark
C. Cain Abel
D. Nessus

Correct Answer: B
Section: (none)
Explanation

QUESTION 195
Which of the following would be MOST important to have to ensure that a company will be able to recover in case of severe environmental trouble or destruction?

A. Disaster recovery plan
B. Alternate sites
C. Offsite storage
D. Fault tolerant systems

Correct Answer: A
Section: (none)
Explanation

QUESTION 196
In a secure environment, which authentication mechanism performs better?

A. RADIUS because it is a remote access authentication service.
B. TACACS because it encrypts client-server negotiation dialogs.
C. RADIUS because it encrypts client-server passwords.
D. TACACS because it is a remote access authentication service.

Correct Answer: B
Section: (none)

Explanation

QUESTION 197
Which of the following common attacks would the attacker capture the user's login information and replay it again later?

A. Back Door Attacks
B. Replay Attack
C. Spoofing
D. Man In The Middle

Correct Answer: C
Section: (none)
Explanation

QUESTION 198
After auditing file, which log will show unauthorized usage attempts?

A. Application
B. Performance
C. Security
D. System

Correct Answer: C
Section: (none)
Explanation

QUESTION 199
Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. Elliptic Curve
B. AES256
C. RSA
D. SHA-1

Correct Answer: C
Section: (none)
Explanation

QUESTION 200
While monitoring application activity and modification, which system should be used?

A. NIDS
B. RADIUS
C. HIDS
D. OVAL

Correct Answer: C
Section: (none)
Explanation

QUESTION 201
The difference between identification and authentication is that:

A. Authentication verifies a set of credentials while identification verifies the identity of the network.
B. Authentication verifies a user ID belongs to a specific user while identification verifies the identity of a user group.
C. Authentication verifies a set of credentials while identification verifies the identity of a user requesting credentials.
D. Authentication verifies the identity of a user requesting credentials while identification verifies a set of credentials.

Correct Answer: C
Section: (none)
Explanation

QUESTION 202
The main objective of risk management in an organization is to reduce risk to a level:

A. Where the ALE is lower than the SLE.
B. Where the ARO equals the SLE.
C. The organization will mitigate.
D. The organization will accept.

Correct Answer: D
Section: (none)
Explanation

QUESTION 203
Following a disaster, which of the following functions should be returned FIRST from the backup facility to the primary facility?

A. Web services
B. Systems functions
C. Executive functions
D. Least critical functions

Correct Answer: D
Section: (none)
Explanation

QUESTION 204
The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. An executive uses PKI to encrypt sensitive emails sent to an assistant. In addition to encrypting the body of the email, the executive wants to encrypt the signature so that the assistant can verify that the email actually came from the executive. Which asymmetric key should be used by the executive to encrypt the signature?

A. Shared
B. Private

C. Hash
D. Public

Correct Answer: B
Section: (none)
Explanation

QUESTION 205
Which of the following is a reason to use a vulnerability scanner?

A. To identify open ports on a system
B. To assist with protocol analyzing
C. To identify remote access policies
D. To assist with PKI implementation

Correct Answer: A
Section: (none)
Explanation

QUESTION 206
Which access control system allows the system administrator to establish access permissions to network resources?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Correct Answer: A
Section: (none)
Explanation

QUESTION 207
Remote authentication allows you to authenticate Zendesk users using a locally hosted script. Which of the following is an example of remote authentication?

A. A user on a metropolitan area network (MAN) accesses a host by entering a username and password pair while not connected to the LAN.
B. A user on a campus area network (CAN) connects to a server in another building and enters a username and password pair.
C. A user in one building logs on to the network by entering a username and password into a host in the same building.
D. A user in one city logs onto a network by connecting to a domain server in another city.

Correct Answer: D
Section: (none)
Explanation

QUESTION 208
Your company's website permits customers to search for a product and display the current price and quantity available of each product from the production database. Which of the following will

invalidate an SQL injection attack launched from the lookup field at the web server level?

A. NIPS
B. Security template
C. Buffer overflow protection
D. Input validation

Correct Answer: D
Section: (none)
Explanation

QUESTION 209
The FIRST step in creating a security baseline would be:

A. Identifying the use case
B. Installing software patches
C. Vulnerability testing.
D. Creating a security policy

Correct Answer: D
Section: (none)
Explanation

QUESTION 210
Look at the following intrusion detection systems carefully, which one uses well defined models of how an attack occurs?

A. Anomaly
B. Protocol
C. Signature
D. Behavior

Correct Answer: C
Section: (none)
Explanation

QUESTION 211
A computer system containing personal identification information is being implemented by a company's sales department. The sales department has requested that the system become operational before a security review can be completed. Which of the following can be used to explain the reasons a security review must be completed?

A. Vulnerability assessment
B. Risk assessment
C. Corporate security policy
D. Need to know policy

Correct Answer: C
Section: (none)
Explanation

QUESTION 212
You work as a network technician. You have been asked to reconstruct the infrastructure of an organization. You should make sure that the virtualization technology is implemented securely. What should be taken into consideration while implementing virtualization technology?

A. The technician should perform penetration testing on all the virtual servers to monitor performance.
B. The technician should verify that the virtual servers and the host have the latest service packs and patches applied.
C. The technician should verify that the virtual servers are dual homed so that traffic is securely separated.
D. The technician should subnet the network so each virtual server is on a different network segment.

Correct Answer: B
Section: (none)
Explanation

QUESTION 213
Which of the following attacks are being referred to if the attack involves the attacker gaining access to a host in the network and logically disconnecting it?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Correct Answer: A
Section: (none)
Explanation

QUESTION 214
.
Which protocol can be used to ensure secure transmissions on port 443?

A. HTTPS
B. SHTTP
C. Telnet
D. SFTP

Correct Answer: A
Section: (none)
Explanation

QUESTION 215
Which of the following protocols is used to transmit data between a web browser and a web server?

A. SSH
B. HTTP
C. SFTP
D. IMAP4

Correct Answer: B
Section: (none)
Explanation

QUESTION 216
Which method can be used to correct a single security issue on a workstation?

A. A patch
B. Configuration baseline
C. A service pack
D. Patch management

Correct Answer: A
Section: (none)
Explanation

QUESTION 217
Which of the following logs shows when the workstation was last shutdown?

A. DHCP
B. Security
C. Access
D. System

Correct Answer: D
Section: (none)
Explanation

QUESTION 218
Documentation describing a group expected minimum behavior is known as:Documentation describing a group? expected minimum behavior is known as:

A. The need to know
B. Acceptable usage
C. The separation of duties
D. A code of ethics

Correct Answer: D
Section: (none)
Explanation

QUESTION 219
Which one of the following options overwrites the return address within a program to execute malicious code?

A. Buffer overflow
B. Rootkit
C. Logic bomb
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

QUESTION 220
Which of the following attacks are being referred to if packets are not connection-oriented and do not require the synchronization process?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Correct Answer: B
Section: (none)
Explanation

QUESTION 221
Which security application can not proactively detect workstation anomalies?

A. HIPS
B. NIDS
C. Antivirus software
D. Personal software firewall.

Correct Answer: B
Section: (none)
Explanation

QUESTION 222
One of the below is a description for a password cracker, which one is it?

A. A program that can locate and read a password file.
B. A program that provides software registration passwords or keys.
C. A program that performs comparative analysis.
D. A program that obtains privileged access to the system.

Correct Answer: C
Section: (none)
Explanation

QUESTION 223
Risk assessment is a common first step in a risk management process. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a

recognized threat (also called hazard). As a best practice, risk assessments should be based upon which of the following?

A. An absolute measurement of threats

B. A qualitative measurement of risk and impact
C. A quantitative measurement of risk, impact and asset value
D. A survey of annual loss, potential threats and asset value

Correct Answer: C
Section: (none)
Explanation

QUESTION 224
Which of the below options would you consider as a program that constantly observes data traveling over a network?

A. Smurfer
B. Sniffer
C. Fragmenter
D. Spoofer

Correct Answer: B
Section: (none)
Explanation

QUESTION 225
Which of the following will require setting a baseline? (Select TWO).

A. Anomaly-based monitoring
B. Signature-based monitoring
C. NIPS
D. Behavior-based monitoring

Correct Answer: AD
Section: (none)
Explanation

QUESTION 226
From the listing of attacks, choose the attack which exploits session initiation between a Transport Control Program (TCP) client and server within a network?

A. Buffer Overflow attack
B. SYN attack
C. Smurf attack
D. Birthday attack

Correct Answer: B
Section: (none)
Explanation

QUESTION 227
Which statement correctly describes the difference between a secure cipher and a secure hash?

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

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 228
Which of the following assessment tools would be MOST appropriate for determining if a password was being sent across the network in clear text?

A. Protocol analyzer
B. Port scanner
C. Password cracker
D. Vulnerability scanner

Correct Answer: A
Section: (none)
Explanation

QUESTION 229
What maybe happen when hashing two different files creates the same result?

A. A mirror
B. A collision
C. A duplication
D. A pseudo-random event

Correct Answer: B
Section: (none)
Explanation

QUESTION 230
A peer-to-peer computer network uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. Which of the following is a security risk while using peer-to-peer software?

A. Licensing
B. Cookies
C. Data leakage
D. Multiple streams

Correct Answer: C
Section: (none)
Explanation

QUESTION 231
From the listing of attacks, which analyzes how the operating system (OS) responds to specific network traffic, in an attempt to determine the operating system running in your networking environment?

A. Operating system scanning.
B. Reverse engineering.
C. Fingerprinting
D. Host hijacking.

Correct Answer: C
Section: (none)
Explanation

QUESTION 232
For the following items, which one is a collection of servers setup to attract hackers?

A. VLAN
B. DMZ
C. Honeynet
D. Honeypot

Correct Answer: C
Section: (none)
Explanation

QUESTION 233
From the listing of attacks, choose the attack which misuses the TCP (Transmission Control Protocol) three-way handshake process, in an attempt to overload network servers, so that authorized users are denied access to network resources?

A. Man in the middle attack
B. Smurf attack
C. Teardrop attack
D. SYN (Synchronize) attack

Correct Answer: D
Section: (none)
Explanation

QUESTION 234
Both the server and the client authenticate before exchanging dat a. This is an example of which of the following?

A. SSO
B. Biometrics
C. Mutual authentication.
D. Multifactor authentication

Correct Answer: C
Section: (none)
Explanation

QUESTION 235
A technician is helping an organization to correct problems with staff members unknowingly

downloading malicious code from Internet websites. Which of the following should the technician do to resolve the problem?

A. Use Java virtual machines to reduce impact
B. Disable unauthorized ActiveX controls
C. Implement a policy to minimize the problem
D. Install a NIDS

Correct Answer: B
Section: (none)
Explanation

QUESTION 236
A protocol analyzer will most likely detect which security related anomalies?

A. Many malformed or fragmented packets
B. Passive sniffing of local network traffic
C. Decryption of encrypted network traffic
D. Disabled network interface on a server

Correct Answer: A
Section: (none)
Explanation

QUESTION 237
One type of network attack sends two different messages that use the same hash function to generate the same message digest. Which network attack does this?

A. Man in the middle attack.
B. Ciphertext only attack.
C. Birthday attack.
D. Brute force attack.

Correct Answer: C
Section: (none)
Explanation

QUESTION 238
In computing, a stateful firewall (any firewall that performs stateful packet inspection (SPI) or stateful inspection) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. You have been studying stateful packet inspection and want to perform this security technique on the network. Which device will you use to BEST utilize stateful packet inspection?

A. Switch
B. Hub
C. IDS
D. Firewall

Correct Answer: D
Section: (none)
Explanation

QUESTION 239
To which of the following viruses does the characteristic when the virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive, form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

Correct Answer: C
Section: (none)
Explanation

QUESTION 240
The DAC (Discretionary Access Control) model has an inherent flaw. Choose the option that describes this flaw.

A. The DAC (Discretionary Access Control) model uses only the identity of the user or specific process to control access to a resource. This creates a security loophole for Trojan horse attacks.
B. The DAC (Discretionary Access Control) model uses certificates to control access to resources. This creates an opportunity for attackers to use your certificates.
C. The DAC (Discretionary Access Control) model does not use the identity of a user to control access to resources. This allows anyone to use an account to access resources.
D. The DAC (Discretionary Access Control) model does not have any known security flaws.

Correct Answer: A
Section: (none)
Explanation

QUESTION 241
The NIC should be placed in which mode to monitor all network traffic while placing a NIDS onto the network?

A. Promiscuous
B. Half-duplex
C. Full-duplex
D. Auto

Correct Answer: A
Section: (none)
Explanation

QUESTION 242
Which of the following is an installable package that includes several patches from the same vendor for various applications?

A. Hotfix
B. Patch template

C. Service pack
D. Patch rollup

Correct Answer: C
Section: (none)
Explanation

QUESTION 243
Which item can be commonly programmed into an application for ease of administration?

A. Back door
B. Trojan
C. Worm
D. Zombie

Correct Answer: A
Section: (none)
Explanation

QUESTION 244
To which of the following viruses does the characteristic when the virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

Correct Answer: A
Section: (none)
Explanation

QUESTION 245
Which of the following is MOST effective in preventing adware?

A. Firewall
B. HIDS
C. Antivirus
D. Pop-up blocker

Correct Answer: D
Section: (none)
Explanation

QUESTION 246
Choose the most effective method of preventing computer viruses from spreading throughout the network.

A. You should require root/administrator access to run programs and applications.
B. You should enable scanning of all e-mail attachments.
C. You should prevent the execution of .vbs files.

D. You should install a host based IDS (Intrusion Detection System)

Correct Answer: B
Section: (none)
Explanation

QUESTION 247
Choose the correct order in which crucial equipment should draw power.

A. Backup generator, UPS battery, UPS line conditioner
B. Uninterruptible Power Supply (UPS) battery, UPS line conditioner, backup generator
C. Backup generator, UPS line conditioner, UPS battery
D. UPS line conditioner, UPS battery, and backup generator

Correct Answer: D
Section: (none)
Explanation

QUESTION 248
Choose the statement that best details the difference between a worm and a Trojan horse?

A. Worms are distributed through e-mail messages while Trojan horses do not.
B. Worms self replicate while Trojan horses do not.
C. Worms are a form of malicious code while Trojan horses are not.
D. There is no difference between a worm and a Trojan horse.

Correct Answer: B
Section: (none)
Explanation

QUESTION 249
Recently, your company has implemented a work from home program. Employees should connect securely from home to the corporate network. Which encryption technology can be used to achieve this goal?

A. L2TP
B. IPSec
C. PPPoE
D. PPTP

Correct Answer: B
Section: (none)
Explanation

QUESTION 250
Choose the statement which best defines the characteristics of a computer virus.

A. A computer virus is a find mechanism, initiation mechanism and can propagate.
B. A computer virus is a learning mechanism, contamination mechanism and can exploit.
C. A computer virus is a search mechanism, connection mechanism and can integrate.
D. A computer virus is a replication mechanism, activation mechanism and has an objective.

Correct Answer: D
Section: (none)
Explanation

QUESTION 251
The CEO of your company is worrying about staff browsing inappropriate material on the Internet via HTTPS. Your company is advised to purchase a product which can decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing. Which type of attack is similar to this product?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 252
After the maximum number attempts have failed, which of the following could set an account to lockout for 30 minutes?

A. Account lockout threshold
B. Account lockout duration
C. Password complexity requirements
D. Key distribution center

Correct Answer: B
Section: (none)
Explanation

QUESTION 253
Choose the attack or malicious code that cannot be prevented or deterred solely through using technical measures.

A. Dictionary attacks.
B. Man in the middle attacks.
C. DoS (Denial of Service) attacks.
D. Social engineering.

Correct Answer: D
Section: (none)
Explanation

QUESTION 254
A Faraday cage or Faraday shield is an enclosure formed by conducting material, or by a mesh of such material. Such an enclosure blocks out external static electrical fields. Faraday cages are named after physicist Michael Faraday, who built one in 1836. Which of the following would a Faraday cage prevent usage of?

A. Cell phone
B. Uninterruptible Power Supply (UPS)
C. Storage drive
D. USB key

Correct Answer: A
Section: (none)
Explanation

QUESTION 255
An Auditing system is necessary to prevent attacks on what part of the system?

A. The files.
B. The operating system.
C. The systems memory
D. None of the above

Correct Answer: A
Section: (none)
Explanation

QUESTION 256
Which encryption algorithm depends on the inability to factor large prime numbers?

A. SHA-1
B. AES256
C. RSA
D. Elliptic Curve

Correct Answer: C
Section: (none)
Explanation

QUESTION 257
Choose the network mapping tool (scanner) which uses ICMP (Internet Control Message Protocol).

A. A port scanner.
B. A map scanner.
C. A ping scanner.
D. A share scanner.

Correct Answer: C
Section: (none)
Explanation

QUESTION 258
Look at the following items, which one usually applies specifically to a web browser?

A. Anti-spyware

B. Pop-up blocker
C. Personal software firewall
D. Antivirus

Correct Answer: B
Section: (none)
Explanation

QUESTION 259
One type of port scan can determine which ports are in a listening state on the network, and can then perform a two way handshake. Which type of port scan can perform this set of actions?

A. A TCP (transmission Control Protocol) SYN (Synchronize) scan
B. A TCP (transmission Control Protocol) connect scan
C. A TCP (transmission Control Protocol) fin scan
D. A TCP (transmission Control Protocol) null scan

Correct Answer: A
Section: (none)
Explanation

QUESTION 260
Which one of the following options will allow for a network to remain operational after a T1 failure?

A. Redundant servers
B. Redundant ISP
C. RAID 5 drive array
D. Uninterruptible Power Supply (UPS)

Correct Answer: B
Section: (none)
Explanation

QUESTION 261
Which of the following has largely replaced SLIP?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Correct Answer: B
Section: (none)
Explanation

QUESTION 262
You work as the network administrator at Certkiller .com. The Certkiller .com network uses the RBAC (Role Based Access Control) model. You must plan the security strategy for users to access resources on the Certkiller .com network. The types of resources you must control access to are mailboxes, and files and printers. Certkiller .com is divided into distinct departments and

functions named Finance, Sales, Research and Development, and Production respectively. Each user has its own workstation, and accesses resources based on the department wherein he/she

works. You must determine which roles to create to support the RBAC (Role Based Access Control) model. Which of the following roles should you create?

A. Create mailbox, and file and printer roles.
B. Create Finance, Sales, Research and Development, and Production roles.
C. Create user and workstation roles.
D. Create allow access and deny access roles.

Correct Answer: B
Section: (none)
Explanation

QUESTION 263
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. Pre-shared keys can be applied to which of the following?

A. TPM
B. PGP
C. Digital signature
D. CA

Correct Answer: B
Section: (none)
Explanation

QUESTION 264
Which of the following definitions fit correctly to RADIUS?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

Correct Answer: D
Section: (none)
Explanation

QUESTION 265
Which description is correct about a tool used by organizations to verify whether or not a staff member has been involved in malicious activity?

A. Mandatory vacations
B. Time of day restrictions

C. Implicit deny
D. Implicit allow

Correct Answer: A
Section: (none)
Explanation

QUESTION 266
Which of the following definitions fit correctly to TACACS?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. It allows credentials to be accepted from multiple methods, including Kerberos.

Correct Answer: D
Section: (none)
Explanation

QUESTION 267
Which access control method gives the owner control over providing permissions?

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

Correct Answer: D
Section: (none)
Explanation

QUESTION 268
Which of the following needs to be backed up on a domain controller to be able to recover Active Directory?

A. System files
B. User date
C. System state
D. Operating system

Correct Answer: C
Section: (none)
Explanation

QUESTION 269
Which item best describes an instance where a biometric system identifies legitimate users as being unauthorized?

A. False acceptance

B. False positive
C. False rejection
D. False negative

Correct Answer: C
Section: (none)
Explanation

QUESTION 270
Which of the following definitions fit correctly to PPTP?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

Correct Answer: A
Section: (none)
Explanation

QUESTION 271
Which one of the following options is an attack launched from multiple zombie machines in attempt to bring down a service?

A. TCP/IP hijacking
B. DoS
C. DDoS
D. Man-in-the-middle

Correct Answer: C
Section: (none)
Explanation

QUESTION 272
From the list of protocols, which two are VPN (Virtual Private Network) tunneling protocols? Choose two protocols.

A. PPP (Point-to-Point Protocol).
B. SLIP (Serial Line Internet Protocol).
C. L2TP (Layer Two Tunneling Protocol).
D. SMTP (Simple Mail Transfer Protocol).
E. PPTP (Point-to-Point Tunneling Protocol).

Correct Answer: CE
Section: (none)
Explanation

QUESTION 273
Sending a patch through a testing and approval process is an example of which option?

A. Acceptable use policies

B. Change management
C. User education and awareness training
D. Disaster planning

Correct Answer: B
Section: (none)
Explanation

QUESTION 274
Which of the following is correct about an instance where a biometric system identifies unauthorized users and allows them access?

A. False positive.
B. False rejection.
C. False acceptance.
D. False negative.

Correct Answer: C
Section: (none)
Explanation

QUESTION 275
You work as the security administrator at Certkiller .com. You must configure the firewall to support TACACS. Which port(s) should you open on the firewall?

A. Port 21
B. Port 161
C. Port 53
D. Port 49

Correct Answer: D
Section: (none)
Explanation

QUESTION 276
Which security measures should be recommended while implementing system logging procedures? (Select TWO).

A. Collect system temporary files.
B. Apply retention policies on the log files.
C. Perform CRC checks.
D. Perform hashing of the log files.

Correct Answer: D
Section: (none)
Explanation

QUESTION 277
Which of the following network attacks cannot occur in an e-mail attack?

A. Dictionary attack

B. Trojan Horse
C. Phage Virus
D. Polymorphic Virus

Correct Answer: A
Section: (none)
Explanation

QUESTION 278
Which media is LEAST susceptible to a tap being placed on the line?

A. Fiber
B. Coaxial
C. UTP
D. STP

Correct Answer: A
Section: (none)
Explanation

QUESTION 279
Which of the following attacks are being referred to if someone is accessing your e-mail server and sending inflammatory information to others?

A. Trojan Horse.
B. Phage Virus.
C. Repudiation Attack.
D. Polymorphic Virus.

Correct Answer: C
Section: (none)
Explanation

QUESTION 280
Tom is a network administrator of his company. He suspects that files are being copied to a remote location during off hours. The file server does not have logging enabled. Which logs will be the BEST place to look for information?

A. Antivirus logs
B. Firewall logs
C. DNS logs
D. Intrusion detection logs

Correct Answer: B
Section: (none)
Explanation

QUESTION 281
A technician is auditing the security posture of an organization. The audit shows that many of the users have the ability to access the company's accounting information. Which of the following should the technician recommend to address this problem?

A. Changing file level audit settings
B. Implementing a host based intrusion detection system
C. Changing the user rights and security groups
D. Implementing a host based intrusion prevention system

Correct Answer: C
Section: (none)
Explanation

QUESTION 282
Job rotation is a cross-training technique where organizations minimize collusion amongst staff.

A. True
B. False

Correct Answer: A
Section: (none)
Explanation

QUESTION 283
A security specialist is reviewing firewall logs and sees the information below. Which of the following BEST describes the attack that is occurring?
s-192.168.0.21:53 --> d-192.168.0.1:0
s-192.168.0.21:53 --> d-192.168.0.1:1
s-192.168.0.21:53 --> d-192.168.0.1:2
s-192.168.0.21:53 --> d-192.168.0.1:3
s-192.168.0.21:53 --> d-192.168.0.1:4
s-192.168.0.21:53 --> d-192.168.0.1:5
s-192.168.0.21:53 --> d-192.168.0.1:6
s-192.168.0.21:53 --> d-192.168.0.1:7
s-192.168.0.21:53 --> d-192.168.0.1:8

A. ARP poisoning
B. DNS spoofing
C. Port scan
D. PING sweep

Correct Answer: C
Section: (none)
Explanation

QUESTION 284
Choose the access control model that allows access control determinations to be performed based on the security labels associated with each user and each data item.

A. MACs (Mandatory Access Control) method
B. RBACs (Role Based Access Control) method
C. LBACs (List Based Access Control) method
D. DACs (Discretionary Access Control) method

Correct Answer: A
Section: (none)

Explanation

QUESTION 285
Which description is true about penetration testing?

A. Simulating an actual attack on a network
B. Establishing a security baseline
C. Hacking into a network for malicious reasons
D. Detecting active intrusions

Correct Answer: A
Section: (none)
Explanation

QUESTION 286
Which of the following would be MOST useful in determining which internal user was the source of an attack that compromised another computer in its network?

A. The firewall's logs
B. The attacking computer's audit logs
C. The target computer's audit logs.
D. The domain controller's logs.

Correct Answer: C
Section: (none)
Explanation

QUESTION 287
Which encryption algorithms can be used to encrypt and decrypt data?

A. NTLM
B. MD5
C. SHA-1
D. RC5

Correct Answer: D
Section: (none)
Explanation

QUESTION 288
By which means do most network bound viruses spread?

A. E-mail
B. Floppy
C. CD-Rom
D. Mass storage devices

Correct Answer: A
Section: (none)
Explanation

QUESTION 289
The Lightweight Directory Access Protocol or LDAP is an application protocol for querying and modifying directory services running over TCP/IP. A user needs to implement secure LDAP on the network. Which port number will secure LDAP use by default?

A. 53
B. 389
C. 443
D. 636

Correct Answer: D
Section: (none)
Explanation

QUESTION 290
Which of the following definitions should BEST suit the functions of an e-mail server?

A. Detect the viruses in the messages received from various sources and send warnings to the recipient to warn him/her of the risky mail.
B. Notify you that a message carries a virus.
C. Forms a platform on which messages are sent.
D. Makes use of a port used specifically for messages to be sent through.

Correct Answer: A
Section: (none)
Explanation

QUESTION 291
On a company's LAN, port 3535 is typically blocked for outbound traffic. An end-user has recently purchased a legitimate business program that needs to make outbound calls through this port. Which step should be taken by a technician to allow this? (Select TWO).

A. Change the users subnet mask.
B. Open the port on the companys firewall.
C. Open the port on the VLAN.
D. Open the port on the users personal software firewall.

Correct Answer: BD
Section: (none)
Explanation

QUESTION 292
Choose the primary disadvantage of using a third party mail relay.

A. Spammers can utilize the third party mail relay.
B. A third party mail relay limits access to specific users.
C. A third party mail relay restricts the types of e-mail that maybe sent.
D. A third party mail relay restricts spammers from gaining access.

Correct Answer: A
Section: (none)

Explanation

QUESTION 293
Which method is the easiest to disable a 10Base2 network?

A. Remove a vampire tap.
B. Introduce crosstalk.
C. Remove a terminator.
D. Install a zombie.

Correct Answer: C
Section: (none)
Explanation

QUESTION 294
Choose the option that details one of the primary benefits of using S/MIME /Secure Multipurpose Internet Mail Extension)?

A. S/MIME allows users to send both encrypted and digitally signed e-mail messages.
B. S/MIME allows users to send anonymous e-mail messages.
C. S/MIME allows users to send e-mail messages with a return receipt.
D. S/MIME expedites the delivery of e-mail messages.

Correct Answer: A
Section: (none)
Explanation

QUESTION 295
For the following items, which is a security limitation of virtualization technology?

A. A compromise of one instance will immediately compromise all instances.
B. It increases false positives on the NIDS.
C. Patch management becomes more time consuming.
D. If an attack occurs, it could potentially disrupt multiple servers.

Correct Answer: D
Section: (none)
Explanation

QUESTION 296
Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) are methods of security management for computers and networks. A HIDS is installed to monitor which of following?

A. Temporary Internet files
B. CPU performance
C. System files
D. NIC performance

Correct Answer: C
Section: (none)

Explanation

QUESTION 297
On the topic of comparing viruses and hoaxes, which statement is TRUE? Choose the best TRUE statement.

A. Hoaxes can create as much damage as a real virus.
B. Hoaxes are harmless pranks and should be ignored.
C. Hoaxes can help educate users about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

Correct Answer: A
Section: (none)
Explanation

QUESTION 298
The purpose of a DNS server is to enable people and applications to lookup records in DNS tables. Why implement security logging on a DNS server?

A. To monitor unauthorized zone transfers
B. To control unauthorized DNS DoS
C. To measure the DNS server performance
D. To perform penetration testing on the DNS server

Correct Answer: A
Section: (none)
Explanation

QUESTION 299
Choose the scheme or system used by PGP (Pretty Good Privacy) to encrypt data.

A. Asymmetric scheme
B. Symmetric scheme
C. Symmetric key distribution system
D. Asymmetric key distribution system

Correct Answer: A
Section: (none)
Explanation

QUESTION 300
Which security threat will affect PCs and can have its software updated remotely by a command and control center?

A. Zombie
B. Adware
C. Worm
D. Virus

Correct Answer: A
Section: (none)

Explanation

QUESTION 301
Which of the following web vulnerabilities is being referred to when it receives more data than it is programmed to accept?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Correct Answer: A
Section: (none)
Explanation

QUESTION 302
Which of the following will permit an administrator to find weak passwords on the network?

A. A password generator
B. A network mapper
C. A hash function
D. A rainbow table

Correct Answer: D
Section: (none)
Explanation

QUESTION 303
Which of the following is a security reason to implement virtualization throughout the network infrastructure?

A. To analyze the various network traffic with protocol analyzers
B. To centralize the patch management of network servers
C. To isolate the various network services and roles
D. To implement additional network services at a lower cost

Correct Answer: C
Section: (none)
Explanation

QUESTION 304
Which security measure should be used while implementing access control?

A. Password complexity requirements
B. Disabling SSID broadcast
C. Time of day restrictions
D. Changing default passwords

Correct Answer: A
Section: (none)
Explanation

QUESTION 305
Which of the following web vulnerabilities is being referred to when it has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers?

A. Buffer Overflows.
B. Cookies.
C. CGI
D. SMTP Relay

Correct Answer: D
Section: (none)
Explanation

QUESTION 306
A company's new employees are asked to sign a document that describes the methods of and purposes for accessing the company's IT systems. Which of the following BEST describes this document?

A. Privacy Act of 1974
B. Authorized Access Policy
C. Due diligence form
D. Acceptable Use Policy

Correct Answer: D
Section: (none)
Explanation

QUESTION 307
Study the following items carefully, which one will permit a user to float a domain registration for a maximum of five days?

A. Spoofing
B. DNS poisoning
C. Domain hijacking
D. Kiting

Correct Answer: D
Section: (none)
Explanation

QUESTION 308
Which of the following definitions BEST suit Java Applet?

A. It is a programming language that allows access to system resources of the system running the script
B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity
D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Correct Answer: B
Section: (none)
Explanation

QUESTION 309
A programmer plans to change the server variable in the coding of an authentication function for a proprietary sales application. Which process should be followed before implementing the new routine on the production application server?

A. Change management
B. Secure disposal
C. Password complexity
D. Chain of custody

Correct Answer: A
Section: (none)
Explanation

QUESTION 310
Which of the following definitions BEST suit Buffer Overflow?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Correct Answer: A
Section: (none)
Explanation

QUESTION 311
An administrator wants to make sure that no equipment is damaged when encountering a fire or false alarm in the server room. Which type of fire suppression system should be used?

A. Carbon Dioxide
B. Deluge sprinkler
C. Hydrogen Peroxide
D. Wet pipe sprinkler

Correct Answer: A
Section: (none)
Explanation

QUESTION 312
An end-to-end traffic performance guarantee made by a service provider to a customer is a:

A. DRP.
B. BCP.
C. SLA.
D. VPN

Correct Answer: C
Section: (none)
Explanation

QUESTION 313
The staff must be cross-trained in different functional areas in order to detect fraud. Which of the following is an example of this?

A. Implicit deny
B. Least privilege
C. Separation of duties
D. Job rotation

Correct Answer: D
Section: (none)
Explanation

QUESTION 314
Which of the following would allow an administrator to find weak passwords on the network?

A. A network mapper
B. A hash function
C. A password generator
D. A rainbow table

Correct Answer: D
Section: (none)
Explanation

QUESTION 315
When power must be delivered to critical systems, which of the following is a countermeasure?

A. Backup generator
B. Warm site
C. Redundant power supplies
D. Uninterruptible power supplies (UPSs)

Correct Answer: A
Section: (none)
Explanation

QUESTION 316
Which of the following statements are true regarding File Sharing?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

Correct Answer: D
Section: (none)
Explanation

QUESTION 317
You work as a network administrator for your company. Taking personal safety into consideration, what fire suppression substances types can effectively prevent damage to electronic equipment?

A. Halon
B. CO
C. Water
D. Foam

Correct Answer: B
Section: (none)
Explanation

QUESTION 318
Which password management system best provides for a system with a large number of users?

A. Self service password reset management systems
B. Locally saved passwords management systems
C. Multiple access methods management systems
D. Synchronized passwords management systems

Correct Answer: A
Section: (none)
Explanation

QUESTION 319
Who is finally in charge of the amount of residual risk?

A. The senior management
B. The DRP coordinator
C. The security technician
D. The organizations security officer

Correct Answer: A
Section: (none)
Explanation

QUESTION 320
Which of the following is the BEST place to obtain a hotfix or patch for an application or system?

A. An email from the vendor
B. A newsgroup or forum
C. The manufacturer's website
D. A CD-ROM

Correct Answer: C

Section: (none)
Explanation

QUESTION 321
Tom is a network administrator of his company. He guesses that PCs on the internal network may be acting as zombies participating in external DDoS attacks. Which item will most effectively confirm the administrators?? suspicions?

A. AV server logs
B. HIDS logs
C. Proxy logs
D. Firewall logs

Correct Answer: D
Section: (none)
Explanation

QUESTION 322
Choose the terminology or concept which best describes a (Mandatory Access Control) model.

A. Lattice
B. Bell La-Padula
C. BIBA
D. Clark and Wilson

Correct Answer: A
Section: (none)
Explanation

QUESTION 323
Password cracking tools are available worldwide over the Internet. Which one of the following items is a password cracking tool?

A. Wireshark
B. Nessus
C. John the Ripper
D. AirSnort

Correct Answer: C
Section: (none)
Explanation

QUESTION 324
Which authentication method does the following sequence: Logon request, encrypts value response, server, challenge, compare encrypts results, authorize or fail referred to?

A. Certificates
B. Security Tokens
C. CHAP
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

QUESTION 325
IDS is short for Intrusion Detection Systems. Which option is the MOST basic form of IDS?

A. Signature
B. Statistical
C. Anomaly
D. Behavioral

Correct Answer: A
Section: (none)
Explanation

QUESTION 326
Which of the following statements is TRUE regarding the Security Token system?

A. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
B. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
C. The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to

authenticate against other principles. This occurs automatically when a request or service is performed by another network.
D. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over

Correct Answer: A
Section: (none)
Explanation

QUESTION 327
Which statement is true about the cryptographic algorithm employed by TLS to establish a session key?

A. Blowfish
B. Diffie-Hellman
C. IKE
D. RSA

Correct Answer: B

Section: (none)
Explanation

QUESTION 328
To aid in preventing the execution of malicious code in email clients, which of the following should be done by the email administrator?

A. Spam and anti-virus filters should be used
B. Regular updates should be performed
C. Preview screens should be disabled
D. Email client features should be disabled

Correct Answer: A
Section: (none)
Explanation

QUESTION 329
Which of the following access control models uses roles to determine access permissions?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

QUESTION 330
Internet filter appliances/servers will most likely analyze which three items? (Select THREE).

A. Certificates
B. CRLs
C. Content
D. URLs

Correct Answer: ACD
Section: (none)
Explanation

QUESTION 331
Which of the following types of publicly accessible servers should have anonymous logins disabled to prevent an attacker from transferring malicious data?

A. FTP
B. Email
C. Web
D. DNS

Correct Answer: A
Section: (none)

Explanation

QUESTION 332
Which practice can best code applications in a secure manner?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 333
In addition to bribery and forgery, which of the following are the MOST common techniques that attackers use to socially engineer people? (Select TWO)

A. Phreaking
B. Dumpster diving
C. Whois search
D. Flattery
E. Assuming a position of authority

Correct Answer: DE
Section: (none)
Explanation

QUESTION 334
Which of the following will restrict access to files according to the identity of the user or group?

A. MAC
B. CRL
C. PKI
D. DAC

Correct Answer: D
Section: (none)
Explanation

QUESTION 335
Which of the following would be an easy way to determine whether a secure web page has a valid certificate?

A. Right click on the lock at the bottom of the browser and check the certificate information
B. Contact Thawte or Verisign and ask about the web page
C. Contact the web page's web master
D. Ensure that the web URL starts with 'https:\\'.

Correct Answer: A
Section: (none)

Explanation

QUESTION 336
Which description is correct concerning the process of comparing cryptographic hash functions of system executables, configuration files, and log files?

A. File integrity auditing
B. Stateful packet filtering
C. Host based intrusion detection
D. Network based intrusion detection

Correct Answer: A
Section: (none)
Explanation

QUESTION 337
A software or hardware device that allows only authorized network traffic in or out of a computer or network is called a:

A. Firewall
B. Packet sniffer
C. Honeypot
D. Anti-virus program

Correct Answer: A
Section: (none)
Explanation

QUESTION 338
While hardening an operating system, which item is LEAST effective?

A. Configuration baselines
B. Limiting administrative privileges
C. Installing HIDS
D. Install a software firewall

Correct Answer: C
Section: (none)
Explanation

QUESTION 339
Which of the following types of attacks is BEST described as an attacker capturing part of a communication and later sending that communication segment to the server while pretending to be the client?

A. TCP/IP hijacking
B. Replay
C. Back door
D. Man in the middle

Correct Answer: B

Section: (none)
Explanation

QUESTION 340
Given: John is a network administrator. He advises the server administrator of his company to implement whitelisting, blacklisting, closing-open relays and strong authentication techniques. Which threat is being addressed?

A. Viruses
B. Adware
C. Spam
D. Spyware

Correct Answer: C
Section: (none)
Explanation

QUESTION 341
Which action should be performed when discovering an unauthorized wireless access point attached to a network?

A. Unplug the Ethernet cable from the wireless access point.
B. Change the SSID on the wireless access point.
C. Run a ping against the wireless access point.
D. Enable MAC filtering on the wireless access point.

Correct Answer: A
Section: (none)
Explanation

QUESTION 342
The risks of social engineering can be decreased by implementing: (Select TWO)

A. Security awareness training
B. Risk assessment policies
C. Operating system patching instructions
D. Vulnerability testing techniques
E. Identity verification methods

Correct Answer: AE
Section: (none)
Explanation

QUESTION 343
When a new network device is configured for first-time installation, which of the following is a security threat?

A. Denial of Service (DoS)
B. Attacker privilege escalation
C. Installation of a back door
D. Use of default passwords

Correct Answer: D
Section: (none)
Explanation

QUESTION 344
Which of the following access control models uses subject and object labels?

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

Correct Answer: A
Section: (none)
Explanation

QUESTION 345
Which of the following access decisions are based on a Mandatory Access Control (MAC) environment?

A. Access control lists
B. Ownership
C. Group membership
D. Sensitivity labels

Correct Answer: D
Section: (none)
Explanation

QUESTION 346
Which tool can best monitor changes to the approved system baseline?

A. Enterprise antivirus software
B. Enterprise performance monitoring software
C. Enterprise key management software
D. Enterprise resource planning software

Correct Answer: B
Section: (none)
Explanation

QUESTION 347
Audit log information can BEST be protected by: (Select TWO).

A. Using a VPN
B. An IDS
C. Access controls that restrict usage
D. An intrusion prevention system (IPS)
E. Recording to write-once media.

F. A firewall that creates an enclave

Correct Answer: CE
Section: (none)
Explanation

QUESTION 348
Which method will most effectively verify that a patch file downloaded from a third party has not been modified since the time that the original manufacturer released the patch?

A. Compare the final MD5 hash with the original.
B. Compare the final LANMAN hash with the original.
C. Download the patch file through a SSL connection.
D. Download the patch file over an AES encrypted VPN connection.

Correct Answer: A
Section: (none)
Explanation

QUESTION 349
Non-essential services are often appealing to attackers because non-essential services: (Select TWO)

A. Consume less bandwidth
B. Are not visible to an IDS
C. Provide root level access
D. Decrease the surface area for the attack
E. Are not typically configured correctly or secured
F. Sustain attacks that go unnoticed

Correct Answer: EF
Section: (none)
Explanation

QUESTION 350
A user downloads and installs a new screen saver and the program starts to rename and delete random files. Which of the following would be the BEST description of this program?

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

Correct Answer: C
Section: (none)
Explanation

QUESTION 351
Which of the following types of malicious software travels across computer networks without requiring a user to distribute the software?

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

Correct Answer: B
Section: (none)
Explanation

QUESTION 352
Which of the following should be done if an audit recording fails in an information system?

A. Log off the user
B. Overwrite the oldest audit records
C. Stop generating audit records
D. Send an alert to the appropriate personnel

Correct Answer: D
Section: (none)
Explanation

QUESTION 353
Many unauthorized staff has been entering the data center by piggybacking authorized staff. The CIO has mandated to stop this behavior. Which technology should be installed at the data center to prevent piggybacking?

A. Mantrap
B. Token access
C. Security badges
D. Hardware locks

Correct Answer: A
Section: (none)
Explanation

QUESTION 354
Which of the following types of authentication BEST describes providing a username, password and undergoing a thumb print scan to access a workstation?

A. Multifactor
B. Mutual
C. Biometric
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

QUESTION 355
Kerberos uses which of the following ports by default?

A. 23
B. 88
C. 139
D. 443

Correct Answer: B
Section: (none)
Explanation

QUESTION 356
What should be taken into consideration while executing proper logging procedures? (Select TWO).

A. The information that is needed to reconstruct events
B. The password requirements for user accounts
C. The virtual memory allocated on the log server
D. The amount of disk space required

Correct Answer: AD
Section: (none)
Explanation

QUESTION 357
In computer programming, DLL injection is a technique used to run code within the address space of another process by forcing it to load a dynamic-link library. Which activity is MOST closely associated with DLL injection?

A. Penetration testing
B. SQL servers
C. Network mapping
D. Vulnerability assessment

Correct Answer: A
Section: (none)
Explanation

QUESTION 358
Which of the following types of cryptography is typically used to provide an integrity check?

A. Public key
B. Asymmetric
C. Symmetric
D. Hash

Correct Answer: D
Section: (none)
Explanation

QUESTION 359
Which description is correct about the standard load for all systems?

A. Configuration baseline
B. Group policy
C. Patch management
D. Security template

Correct Answer: A
Section: (none)
Explanation

QUESTION 360
Which of the following authentication systems make use of the KDC Key Distribution Center?

A. Certificates
B. Security Tokens
C. CHAP
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: