SY0-001

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Security+

Version 2.0

Important Note, Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the TestKing web site for an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Login** (upper right corner)
3. Enter e-mail and password
4. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state

1. Exam number and version.
2. Question number.
3. Order number and login ID.

Our experts will answer your mail promptly.

Explanations
Currently this product does not include explanations. If you are interested in providing TestKing with explanations contact feedback@testking.com. Include the following information: exam, your background regarding this exam in particular, and what you consider a reasonable compensation for the work.

Copyright

QUESTION NO: 1
The best protection against the abuse of remote maintenance of PBX (Private Branch Exchange) system is to:

A. Keep maintenance features turned off until needed
B. Insists on strong authentication before allowing remote maintenance
C. Keep PBX (Private Branch Exchange) in locked enclosure and restrict access to only a few people.
D. Check to see if the maintenance caller is on the list of approved maintenance personnel

Answer: B

QUESTION NO: 2
A high profile company has been receiving a high volume of attacks on their web site. The network administrator wants to be able to collect information on the attacker(s) so legal action can be taken.
What should be implemented?

A. A DMZ (Demilitarized Zone)
B. A honey pot
C. A firewall
D. A new subnet

Answer: B

QUESTION NO: 3
The protection of data against unauthorized access or disclosure is an example of what?

A. Confidentiality
B. Integrity
C. Signing
D. Hashing

Answer: A

QUESTION NO: 4
You are running cabling for a network through a boiler room where the furnace and some other heavy machinery reside. You are concerned about interference from these sources.
Which of the following types of cabling provides the best protection from interference in this area?

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

Answer: D

QUESTION NO: 5
In order for a user to obtain a certificate from a trusted CA (Certificate Authority), the user must present proof of identity and a:

A. Private key
B. Public key
C. Password
D. Kerberos key

Answer: B

QUESTION NO: 6
If a private key becomes compromised before its certificate's normal expiration, X.509 defines a method requiring each CA (Certificate Authority) to periodically issue a signed data structure called a certificate:

A. Enrollment list
B. Expiration list
C. Revocation list
D. Validation list

Answer: C

QUESTION NO: 7
An application that appears to perform a useful function but instead contains some sort of malicious code is called a _____.

A. Worm
B. SYN flood
C. Virus
D. Trojan Horse
E. Logic Bomb

Answer: D

QUESTION NO: 8
How many bits are employed when using has encryption?

A. 32
B. 64
C. 128
D. 256

Answer: C

QUESTION NO: 9
What transport protocol and port number does SHH (Secure Shell) use?

A. TCP (Transmission Control Protocol) port 22
B. UDP (User Datagram Protocol) port 69
C. TCP (Transmission Control Protocol) port 179
D. UDP (User Datagram Protocol) port 17

Answer: A

QUESTION NO: 10
While performing a routing site audit of your wireless network, you discover an unauthorized Access Point placed on your network under the desk of Accounting

department security. When questioned, she denies any knowledge of it, but informs you that her new boyfriend has been to visit her several times, including taking her to lunch one time.
What type of attack have you just become a victim of?

A. SYN Flood.
B. Distributed Denial of Service.
C. Man in the Middle attack.
D. TCP Flood.
E. IP Spoofing.
F. Social Engineering
G. Replay attack
H. Phone tag
I. Halloween attack

Answer: F

QUESTION NO: 11
When visiting an office adjacent to the server room, you discover the lock to the window is broken. Because it is not your office you tell the resident of the office to contact the maintenance person and have it fixed. After leaving, you fail to follow up on whether the windows was actually repaired.
What affect will this have on the likelihood of a threat associated with the vulnerability actually occurring?

A. If the window is repaired, the likelihood of the thread occurring will increase.
B. If the window is repaired, the likelihood of the threat occurring will remain constant.
C. If the window is not repaired the, the likelihood of the threat occurring will decrease.
D. If the window is not repaired, the likelihood of the threat occurring will increase.

Answer: D

QUESTION NO: 12
Providing false information about the source of an attack is known as:

A. Aliasing
B. Spoofing
C. Flooding

D. Redirecting

Answer: B

QUESTION NO: 13
The start of the LDAP (Lightweight Directory Access Protocol) directory is called the:

A. Head
B. Root
C. Top
D. Tree

Answer: B

QUESTION NO: 14
A company consists of a main building with two smaller branch offices at opposite ends of the city. The main building and branch offices are connected with fast links so that all employees have good connectivity to the network.
Each of the buildings has security measures that require visitors to sign in, and all employees are required to wear identification badges at all times. You want to protect servers and other vital equipment so that the company has the best level of security at the lowest possible cost.
Which of the following will you do to achieve this objective?

A. Centralize servers and other vital components in a single room of the main building, and add security measures to this room so that they are well protected.
B. Centralize most servers and other vital components in a single room of the main building, and place servers at each of the branch offices. Add security measures to areas where the servers and other components are located.
C. Decentralize servers and other vital components, and add security measures to areas where the servers and other components are located.
D. Centralize servers and other vital components in a single room in the main building. Because the building prevents unauthorized access to visitors and other persons, there is no need to implement physical security in the server room.

Answer: A

QUESTION NO: 15
You are explaining SSL to a junior administrator and come up to the topic of handshaking.
How many steps are employed between the client and server in the SSL handshake process?

A. Five
B. Six
C. Seven
D. Eight

Answer: B

QUESTION NO: 16
An administrator notices that an e-mail server is currently relaying e-mail (including spam) for any e-mail server requesting relaying. Upon further investigation the administrator notices the existence of /etc/mail/relay domains. What modifications should the administrator make to the relay domains file to prevent relaying for non-explicitly named domains?

A. Move the .* entry to the bottom of the relay domains file and restart the e-mail process.
B. Move the .* entry to the top of the relay domains file and restart the e-mail process.
C. Delete the .* entry in the relay domains file and restart the e-mail process.
D. Delete the relay domains file from the /etc/mail folder and restart the e-mail process.

Answer: C

QUESTION NO: 17
Access control decisions are based on responsibilities that an individual user or process has in an organization.
This best describes:

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. DAC (Discretionary Access Control)
D. None of the above.

Answer: B

QUESTION NO: 18
A honey pot is _____.

A. A false system or network to attract attacks away from your real network.
B. A place to store passwords.
C. A sage haven for your backup media.
D. Something that exist only in theory.

Answer: A

QUESTION NO: 19
A problem with air conditioning is causing fluctuations in temperature in the server room. The temperature is rising to 90 degrees when the air conditioner stops working, and then drops to 60 degrees when it starts working again.
The problem keeps occurring over the next two days.
What problem may result from these fluctuations? (Select the best answer)

A. Electrostatic discharge
B. Power outages
C. Chip creep
D. Poor air quality

Answer: C

QUESTION NO: 20
You have been alerted to the possibility of someone using an application to capture and manipulate packets as they are passing through your network.
What type of threat does this represent?

A. DDos
B. Back Door
C. Spoofing
D. Man in the Middle

Answer: D

QUESTION NO: 21
Which of the following media types is most immune to RF (Radio Frequency) eavesdropping?

A. Coaxial cable
B. Fiber optic cable
C. Twisted pair wire
D. Unbounded

Answer: B

QUESTION NO: 22
What statement is most true about viruses and hoaxes?

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 user about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

Answer: A

QUESTION NO: 23
While connected from home to an ISP (Internet Service Provider), a network administrator performs a port scan against a corporate server and encounters four open TCP (Transmission Control Protocol) ports: 25, 110, 143 and 389. Corporate users in the organization must be able to connect from home, send and receive messages on the Internet, read e-mail by beams of the IMAPv.4 (Internet Message Access Protocol version 4) protocol, and search into a directory services database for user e-mail addresses, and digital certificates. All the e-mail relates services, as well as the directory server, run on the scanned server.
Which of the above ports can be filtered out to decrease unnecessary exposure without affecting functionality?

A. 25

B. 110
C. 143
D. 389

Answer: B

QUESTION NO: 24
A piece of malicious code that can replicate itself has no productive purpose and exist only to damage computer systems or create further vulnerabilities is called a?

A. Logic Bomb
B. Worm
C. Trojan Horse
D. SYN flood
E. Virus

Answer: E

QUESTION NO: 25
When evidence is acquired, a log is started that records who had possession of the evidence for a specific amount of time. This is to avoid allegations that the evidence may have been tampered with when it was unaccounted for, and to keep track of the tasks performed in acquiring evidence from a piece of equipment or materials. What is the term used to describe this process?

A. Chain of command.
B. Chain of custody.
C. Chain of jurisdiction.
D. Chain of evidence.

Answer: B

QUESTION NO: 26
Data integrity is best achieved using a(n)

A. Asymmetric cipher
B. Digital certificate

C. Message digest
D. Symmetric cipher

Answer: C

QUESTION NO: 27
A recent audit shows that a user logged into a server with their user account and executed a program. The user then performed activities only available to an administrator.
This is an example of an attack?

A. Trojan horse
B. Privilege escalation
C. Subseven back door
D. Security policy removal

Answer: B

QUESTION NO: 28
When a user clicks to browse a secure page, the SSL (Secure Sockets Layer) enabled server will first:

A. Use its digital certificate to establish its identity to the browser.
B. Validate the user by checking the CRL (Certificate Revocation List).
C. Request the user to produce the CRL (Certificate Revocation List).
D. Display the requested page on the browser, then provide its IP (Internet Protocol) address for verification

Answer: A

QUESTION NO: 29
You are assessing risks and determining which asset protection policies to create first. Another member of the IT staff has provided you with a list of assets which have importance weighted on a scale of 1 to 10. Internet connectivity has an importance of 8, data has an importance of 9, personnel have an importance of 7, and software has an importance of 5.
Based on the weights, what is the order in which you will generate new policies?

A. Internet policy, data security, personnel safety policy, software policy.
B. Data security policy, Internet policy, software policy, personnel safety policy.
C. Software policy, personnel safety policy, Internet policy, data security policy.
D. Data security policy, Internet policy, personnel safety policy, software policy.

Answer: D

QUESTION NO: 30
Controlling access to information systems and associated networks is necessary for the preservation of their:

A. Authenticity, confidentiality, integrity and availability.
B. Integrity and availability.
C. Confidentiality, integrity and availability.
D. Authenticity, confidentiality and availability.

Answer: C

QUESTION NO: 31
What design feature of Instant Messaging makes it extremely insecure compared to other messaging systems?

A. It is a peer-to-peer network that offers most organizations virtually no control over it.
B. Most IM clients are actually Trojan Horses.
C. It is a centrally managed system that can be closely monitored.
D. It uses the insecure Internet as a transmission medium.

Answer: A

QUESTION NO: 32
Access controls that are created and administered by the data owner are considered:

A. MACs (Mandatory Access Control)
B. RBACs (Role Based Access Control)

C. LBACs (List Based Access Control)
D. DACs (Discretionary Access Control)

Answer: D

QUESTION NO: 33
A well defined business continuity plan must consist of risk and analysis, business impact analysis, strategic planning and mitigation, training and awareness, maintenance and audit and:

A. Security labeling and classification.
B. Budgeting and acceptance.
C. Documentation and security labeling.
D. Integration and validation.

Answer: D

QUESTION NO: 34
John wants to encrypt a sensitive message before sending it to one of his managers. Which type of encryption is often used for e-mail?

A. S/MINE
B. BIND
C. DES
D. SSL

Answer: A

QUESTION NO: 35
What is the greatest benefit to be gained through the use of S/MINE /Secure Multipurpose Internet Mail Extension) The ability to:

A. Encrypted and digitally sign e-mail messages.
B. Send anonymous e-mails.
C. Send e-mails with a return receipt.
D. Expedite the delivery of e-mail.

Answer: A

QUESTION NO: 36
A _____ occurs when a string of data is sent to a buffer that is larger than the buffer was designed to handle.

A. Brute Force attack
B. Buffer owerflow
C. Man in the middle attack
D. Blue Screen of Death
E. SYN flood
F. Spoofing attack

Answer: B

QUESTION NO: 37
Packet sniffing can be used to obtain username and password information in clear text from which one of the following?

A. SSH (Secure Shell)
B. SSL (Secure Sockets Layer)
C. FTP (File Transfer Protocol)
D. HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)

Answer: C

QUESTION NO: 38
A company uses WEP (Wired Equivalent Privacy) for wireless security.
Who may authenticate to the company's access point?

A. Only the administrator.
B. Anyone can authenticate.
C. Only users within the company.
D. Only users with the correct WEP (Wired Equivalent Privacy) key.

Answer: D

QUESTION NO: 39
As the Security Analyst for your companies network, you become aware that your systems may be under attack. This kind of attack is a DOS attack and the exploit send more traffic to a node than anticipated.
What kind of attack is this?

A. Ping of death
B. Buffer Overflow
C. Logic Bomb
D. Smurf

Answer: B

QUESTION NO: 40
Following a disaster, while returning to the original site from an alternate site, the first process to resume at the original site would be the:

A. Least critical process
B. Most critical process.
C. Process most expensive to maintain at an alternate site.
D. Process that has a maximum visibility in the organization.

Answer: A

QUESTION NO: 41
In order to establish a secure connection between headquarters and a branch office over a public network, the router at each location should be configured to use IPSec (Internet Protocol Security) in _____ mode.

A. Secure
B. Tunnel
C. Transport
D. Data link

Answer: B

QUESTION NO: 42
The primary purpose of NAT (Network Address Translation) is to:

A. Translate IP (Internet Protocol) addresses into user friendly names.
B. Hide internal hosts from the public network.
C. Use on public IP (Internet Protocol) address on the internal network as a name server.
D. Hide the public network from internal hosts.

Answer: B

QUESTION NO: 43
Users of Instant Messaging clients are especially prone to what?

A. Theft of root user credentials.
B. Disconnection from the file server.
C. Hostile code delivered by file transfer.
D. Slow Internet connections.
E. Loss of email privileges.
F. Blue Screen of Death errors.

Answer: C

QUESTION NO: 44
Which two of the following are symmetric-key algorithms used for encryption?

A. Stream-cipher
B. Block
C. Public
D. Secret

Answer: A, B

QUESTION NO: 45

Computer forensics experts collect and analyze data using which of the following guidelines so as to minimize data loss?

A. Evidence
B. Chain of custody
C. Chain of command
D. Incident response

Answer: B

QUESTION NO: 46
A DMZ (Demilitarized Zone) typically contains:

A. A customer account database
B. Staff workstations
C. A FTP (File Transfer Protocol) server
D. A SQL (Structured Query Language) based database server

Answer: C

QUESTION NO: 47
What kind of attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss but the lack of legitimate use of that system?

A. CRL
B. DOS
C. ACL
D. MD2

Answer: B

QUESTION NO: 48
User A needs to send a private e-mail to User B. User A does not want anyone to have the ability to read the e-mail except for User B, thus retaining privacy. Which tenet of information security is User A concerned about?

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

Answer: C

QUESTION NO: 49
You are researching the ARO and need to find specific data that can be used for risk assessment.
Which of the following will you use to find information?

A. Insurance companies
B. Stockbrokers
C. Manuals included with software and equipment.
D. None of the above. There is no way to accurately predict the ARO.

Answer: A

QUESTION NO: 50
Giving each user or group of users only the access they need to do their job is an example of which security principal.

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

Answer: A

QUESTION NO: 51
Documenting change levels and revision information is most useful for:

A. Theft tracking
B. Security audits
C. Disaster recovery
D. License enforcement

Answer: C

QUESTION NO: 52
One way to limit hostile sniffing on a LAN (Local Area Network is by installing:

A. An ethernet switch.
B. An ethernet hub.
C. A CSU/DSU (Channel Service Unit/Data Service Unit).
D. A firewall.

Answer: A

QUESTION NO: 53
Notable security organizations often recommend only essential services be provided by a particular host, and any unnecessary services be disable.
Which of the following does NOT represent a reason supporting this recommendation?

A. Each additional service increases the risk of compromising the host, the services that run on the host, and potential clients of these services.
B. Different services may require different hardware, software, or a different discipline of administration.
C. When fewer services and applications are running on a specific host, fewer log entries and fewer interactions between different services are expected, which simplifies the analysis and maintenance of the system from a security point of view.
D. If a service is not using a well known port, firewalls will not be able to disable access to this port, and an administrator will not be able to restrict access to this service.

Answer: D

QUESTION NO: 54
Which of the following backup methods copies only modified files since the last full backup?

A. Full
B. Differential
C. Incremental
D. Archive

Answer: B

QUESTION NO: 55
You are compiling estimates on how much money the company could lose if a risk occurred one time in the future.
Which of the following would these amounts represent?

A. ARO
B. SLE
C. ALE
D. Asset identification

Answer: B

QUESTION NO: 56
The term "due care" best relates to:

A. Policies and procedures intended to reduce the likelihood of damage or injury.
B. Scheduled activity in a comprehensive preventative maintenance program.
C. Techniques and methods for secure shipment of equipment and supplies.
D. User responsibilities involved when sharing passwords in a secure environment.

Answer: A

QUESTION NO: 57
Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies.
What type of encryption is it from the list below?

A. WTLS
B. Symmetric
C. Multifactor

D. Asymmetric

Answer: B

QUESTION NO: 58
You are the first person to respond to the scene of an incident involving a computer being hacked. After determining the scope of the crime scene and securing it, you attempt to preserve evidence at the scene.
Which of the following tasks will you perform to preserve evidence? (Choose all that apply)

A. Photograph any information displayed on the monitors of computers involved in the incident.
B. Document any observation or messages displayed by the computer.
C. Shut down the computer to prevent further attacks that may modify data.
D. Gather up manuals, nonfunctioning devices, and other materials and equipment in the area so they are ready for transport.

Answer: A, B

QUESTION NO: 59
At what stage of an assessment would an auditor test systems for weaknesses and attempt to defeat existing encryption, passwords and access lists?

A. Penetration
B. Control
C. Audit planning
D. Discovery

Answer: A

QUESTION NO: 60
When examining the server's list of protocols that are bound and active on each network interface card, the network administrator notices a relatively large number of protocols.
Which actions should be taken to ensure network security?

A. Unnecessary protocols do not pose a significant to the system and should be left intact for compatibility reasons.
B. There are no unneeded protocols on most systems because protocols are chosen during the installation.
C. Unnecessary protocols should be disable on all server and client machines on a network as they pose great risk.
D. Using port filtering ACLs (Access Control List) at firewalls and routers is sufficient to stop malicious attacks on unused protocols.

Answer: C

QUESTION NO: 61
Which of the following describes the concept of data integrity?

A. A means of determining what resources a user can use and view.
B. A method of security that ensures all data is sequenced, and numbered.
C. A means of minimizing vulnerabilities of assets and resources.
D. A mechanism applied to indicate a data's level of security.

Answer: B

QUESTION NO: 62
In a decentralized privilege management environment, user accounts and passwords are stored on:

A. One central authentication server.
B. Each individual server.
C. No more than two servers.
D. One server configured for decentralized management.

Answer: B

QUESTION NO: 63
In context of wireless networks, WEP (Wired Equivalent Privacy) was designed to:

A. Provide the same level of security as a wired LAN (Local Area Network).
B. Provide a collision preventive method of media access.

C. Provide a wider access area that that of wired LANs (Local Area Network).
D. Allow radio frequencies to penetrate walls.

Answer: A

QUESTION NO: 64
What two functions does IPSec perform? (Choose two)

A. Provides the Secure Shell (SSH) for data confidentiality.
B. Provides the Password Authentication Protocol (PAP) for user authentication.
C. Provides the Authentication Header (AH) for data integrity.
D. Provides the Internet Protocol (IP) for data integrity.
E. Provides the Nonrepudiation Header (NH) for identity integrity.
F. Provides the Encapsulation Security Payload (ESP) for data confidentiality.

Answer: C, F

QUESTION NO: 65
A primary drawback to using shared storage clustering for high availability and disaster recover is:

A. The creation of a single point of vulnerability.
B. The increased network latency between the host computers and the RAID (Redundant Array of Independent Disk) subsystem.
C. The asynchronous writes which must be used to flush the server cache.
D. The highest storage capacity required by the RAID (Redundant Array of Independent Disks) subsystem.

Answer: A

QUESTION NO: 66
What are two common methods when using a public key infrastructure for maintaining access to servers in a network?

A. ACL and PGP.
B. PIM and CRL.
C. CRL and OCSP.

D. RSA and MD2

Answer: C

QUESTION NO: 67
After installing a new operating system, what configuration changes should be implemented?

A. Create application user accounts.
B. Rename the guest account.
C. Rename the administrator account, disable the guest accounts.
D. Create a secure administrator account.

Answer: C

QUESTION NO: 68
Users who configure their passwords using simple and meaningful things such as pet names or birthdays are subject to having their account used by an intruder after what type of attack?

A. Dictionary attack
B. Brute Force attack
C. Spoofing attack
D. Random guess attack
E. Man in the middle attack
F. Change list attack
G. Role Based Access Control attack
H. Replay attack
I. Mickey Mouse attack

Answer: A

QUESTION NO: 69
By definition, how many keys are needed to lock and unlock data using symmetric-key encryption?

A. 3+

B. 2
C. 1
D. 0

Answer: C

QUESTION NO: 70
What kind of attack are hashed password vulnerable to?

A. Man in the middle.
B. Dictionary or brute force.
C. Reverse engineering.
D. DoS (Denial of Service)

Answer: B

QUESTION NO: 71
What is one advantage if the NTFS file system over the FAT16 and FAT32 file systems?

A. Integral support for streaming audio files.
B. Integral support for UNIX compatibility.
C. Integral support for dual-booting with Red Hat Linux.
D. Integral support for file and folder level permissions.

Answer: D

QUESTION NO: 72
You have identified a number of risks to which your company's assets are exposed, and want to implement policies, procedures, and various security measures. In doing so, what will be your objective?

A. Eliminate every threat that may affect the business.
B. Manage the risks so that the problems resulting from them will be minimized.
C. Implement as many security measures as possible to address every risk that an asset may be exposed to.
D. Ignore as many risks as possible to keep costs down.

Answer: B

QUESTION NO: 73
Which of the following results in a domain name server resolving the domain name to a different and thus misdirecting Internet traffic?

A. DoS (Denial of Service)
B. Spoofing
C. Brure force attack
D. Reverse DNS (Domain Name Service)

Answer: B

QUESTION NO: 74
Active detection IDS systems may perform which of the following when a unauthorized connection attempt is discovered? (Choose all that apply)

A. Inform the attacker that he is connecting to a protected network.
B. Shut down the server or service.
C. Provide the attacker the usernames and passwords for administrative accounts.
D. Break of suspicious connections.

Answer: B, D

QUESTION NO: 75
Honey pots are useful in preventing attackers from gaining access to critical system. True or false?

A. True
B. False
C. It depends on the style of attack used.

Answer: A

QUESTION NO: 76
A autonomous agent that copies itself into one or more host programs, then propagates when the host is run, is best described as a:

A. Trojan horse
B. Back door
C. Logic bomb
D. Virus

Answer: D

QUESTION NO: 77
What technology was originally designed to decrease broadcast traffic but is also beneficial in reducing the likelihood of having information compromised by sniffers?

A. VPN (Virtual Private Network)
B. DMZ (Demilitarized Zone)
C. VLAN (Virtual Local Area Network)
D. RADIUS (Remote Authentication Dial-in User Service)

Answer: C

QUESTION NO: 78
Of the following services, which one determines what a user can change or view?

A. Data integrity
B. Data confidentiality
C. Data authentication
D. Access control

Answer: D

QUESTION NO: 79
IMAP4 requires port ____ to be open.

A. 80
B. 3869
C. 22
D. 21
E. 23
F. 25
G. 110
H. 143
I. 443

Answer: H

QUESTION NO: 80
What are access decisions based on in a MAC (Mandatory Access Control) environment?

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

Answer: D

QUESTION NO: 81
As the Security Analyst for your companies network, you want to implement AES. What algorithm will it use?

A. Rijndael
B. Nagle
C. Spanning Tree
D. PKI

Answer: A

QUESTION NO: 82
When securing a FTP (File Transfer Protocol) server, what can be done to ensure that only authorized users can access the server?

A. Allow blind authentication.
B. Disable anonymous authentication.
C. Redirect FTP (File Transfer Protocol) to another port.
D. Only give the address to users that need access.

Answer: B

QUESTION NO: 83
Asymmetric cryptography ensures that:

A. Encryption and authentication can take place without sharing private keys.
B. Encryption of the secret key is performed with the fastest algorithm available.
C. Encryption occurs only when both parties have been authenticated.
D. Encryption factoring is limited to the session key.

Answer: A

QUESTION NO: 84
You are promoting user awareness in forensics, so users will know what to do when incidents occur with their computers.
Which of the following tasks should you instruct users to perform when an incident occurs? (Choose all that apply)

A. Shut down the computer.
B. Contact the incident response team.
C. Documents what they see on the screen.
D. Log off the network.

Answer: B, C

QUESTION NO: 85
When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exist to handle the usually rapid "hand-shaking" exchange of messages that sets up the session.
What kind of attack exploits this functionality?

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

Answer: B

QUESTION NO: 86
A program that can infect other programs by modifying them to include a version of itself is a:

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

Answer: B

QUESTION NO: 87
A collection of information that includes login, file access, other various activities, and actual or attempted legitimate and unauthorized violations is a(n):

A. Audit
B. ACL (Access Control List)
C. Audit trail
D. Syslog

Answer: C

QUESTION NO: 88
Forensic procedures must be followed exactly to ensure the integrity of data obtained in an investigation. When making copies of data from a machine that us being examined, which of the following tasks should be done to ensure it is an exact duplicate?

A. Perform a cyclic redundancy check using a checksum or hashing algorithm.
B. Change the attributes of data to make it read only.

C. Open files on the original media and compare them to the copied data.
D. Do nothing. Imaging software always makes an accurate image.

Answer: A

QUESTION NO: 89
DAC (Discretionary Access Control) system operate which following statement:

A. Files that don't have an owner CANT NOT be modified.
B. The administrator of the system is an owner of each object.
C. The operating system is an owner of each object.
D. Each object has an owner, which has full control over the object.

Answer: D

QUESTION NO: 90
You have decided to implement biometrics as part of your security system. Before purchasing a locking system that uses biometrics to control access to secure areas, you need to decide what will be used to authenticate users.
Which of the following options relies solely on biometric authentication?

A. Username and password.
B. Fingerprints, retinal scans, PIN numbers, and facial characteristics.
C. Voice patterns, fingerprints, and retinal scans.
D. Strong passwords, PIN numbers, and digital imaging.

Answer: C

QUESTION NO: 91
As the Security Analyst for your companies network, you want to implement Single Signon technology.
What benefit can you expect to get when implementing Single Signon?

A. You will need to log on twice at all times.
B. You can allow for system wide permissions with it.
C. You can install multiple applications.
D. You can browse multiple directories.

Answer: D

QUESTION NO: 92
Many intrusion detection systems look for known patterns or _____ to aid in detecting attacks.

A. Viruses
B. Signatures
C. Hackers
D. Malware

Answer: B

QUESTION NO: 93
What type of authentication may be needed when a stored key and memorized password are not strong enough and additional layers of security is needed?

A. Mutual
B. Multi-factor
C. Biometric
D. Certificate

Answer: B

QUESTION NO: 94
You are the first to arrive at a crime scene in which a hacker is accessing unauthorized data on a file server from across the network.
To secure the scene, which of the followings actions should you perform?

A. Prevent members of the organization from entering the server room.
B. Prevent members of the incident response team from entering the server room.
C. Shut down the server to prevent the user from accessing further data.
D. Detach the network cable from the server to prevent the user from accessing further data.

Answer: A, D

QUESTION NO: 95
You are the first person to arrive at a crime scene. An investigator and crime scene technician arrive afterwards to take over the investigation.
Which of the following tasks will the crime scene technician be responsible for performing?

A. Ensure that any documentation and evidence they possessed is handled over to the investigator.
B. Reestablish a perimeter as new evidence presents itself.
C. Establish a chain of command.
D. Tag, bag, and inventory evidence.

Answer: D

QUESTION NO: 96
The defacto IT (Information Technology) security evaluation criteria for the international community is called?

A. Common Criteria
B. Global Criteria
C. TCSEC (Trusted Computer System Evaluation Criteria)
D. ITSEC (Information Technology Security Evaluation Criteria)

Answer: A

QUESTION NO: 97
Which of the following is a technical solution that supports high availability?

A. UDP (User Datagram Protocol)
B. Anti-virus solution
C. RAID (Redundant Array of Independent Disks)
D. Firewall

Answer: C

QUESTION NO: 98
Which of the following is an example of an asymmetric algorithm?

A. CAST (Carlisle Adams Stafford Tavares)
B. RC5 (Rivest Cipher 5)
C. RSA (Rivest Shamir Adelman)
D. SHA-1 (Secure Hashing Algorithm 1)

Answer: C

QUESTION NO: 99
Dave is increasing the security of his Web site by adding SSL (Secure Sockets Layer).
Which type of encryption does SSL use?

A. Asymmetric
B. Symmetric
C. Public Key
D. Secret

Answer: B