CertifyMe

Number: SY0-101
Passing Score: 800
Time Limit: 120 min
File Version: 7.5

http://www.gratisexam.com/

CertifyMe SY0-101

Exam A

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Checking with various outside opinions, answer A would be the best.

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: A deception active response fools the attacker into thinking the attack is succeeding while monitoring the activity and potentially redirecting the attacker to a system that is designed to be broken. This allows the operator or administrator to gather data about how the attack is unfolding and what techniques are being used in the attack. This process is referred to as sending them to the honey pot. Reference: Security + (SYBEX) page 183

QUESTION 3
prevent or minimize unauthorized access and disclosure of data and information is:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: The goal of confidentiality is to prevent or minimize unauthorized access and disclosure of data and information.
Reference: Security + (SYBEX) page 22

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fiber, as a media, is relatively secure because it cannot be easily tapped. It is the strongest to defeat against EMI
and RFI in my opinion.
Reference: Security + (SYBEX) page 147

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A certificate is really nothing more than a mechanism that associates the public key with an individual.
Reference: Security + (SYBEX) page 332

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Certification revocation is the process of revoking a certification before it expires. A certificate may need to be revoked because it was stolen, an employee moved on to a new company, or someone has had their access revoked.
Reference: Security + (SYBEX) page 337

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for free game, software, or other file.
Reference: Security + (SYBEX) page 80

QUESTION 8
How many bits are employed when using has encryption?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 183

QUESTION 9
What transport protocol and port number does SSH (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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SSH uses port 22 and TCP for connections.
Reference: Security + (SYBEX) page 127

QUESTION 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

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, be e-mail, or by a visit.
Reference: Security + (SYBEX) page 87

QUESTION 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 threat 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is the only answer that can be true.
A. Is false, because why would a repair of the door increase the threat.
B. Is false, because a repair, there is no vulnerability.

C. If the window is not repaired, then the threat will increase not decrease.

QUESTION 12
Providing false information about the source of an attack is known as:

A. Aliasing
B. Spoofing
C. Flooding
D. Redirecting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A spoofing attack is simple an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack.
Reference: Security + (SYBEX) page 56

QUESTION 13
The start of the LDAP (Lightweight Directory Access Protocol) directory is called the:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
LDAP directories are arranged as trees. Below the topmost 'root' node, country information appears, followed by entries for companies, states or national organizations. Next come entries for organizational units, such as branch offices and departments. Finally we locate individuals, which inX.500 and LDAP include people, shared resources such as printers, and documents. An LDAP directory server thus makes it possible for a corporate user to find the information resources she needs anywhere on the enterprise network.
Reference: http://www.intranetjournal.com/foundation/ldap.shtml

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Keep in mind that cost and best level of security is asked for. To keep all the servers in one room along with the vital components with a security measure added to the room will provide what is asked for.

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Graphical explanation of 6 steps to Digital Handshake for SSL Note: The handshake begins when a browser connects to an SSL-enabled server, and asks the server to send back its identification, a digital certificate that usually contains the server name, the trusted certifying authority, and the server public encryption key. The browser can contact the server of the trusted certifying authority and confirm that the certificate is authentic before proceeding.The browser then presents a list of encryption algorithms and hashing functions (used to generate a number
from another); the server picks the strongest encryption that it also supports and notifies the client of the decision In order to generate the session keys used for the secure connection, the browser uses the server public
key from the certificate to encrypt a random number and send it to the server. The client can encrypt this data, but only the server can decrypt it: this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data
The server replies with more random data (which doesn't have to be encrypted), and then both parities use the selected hash functions on the random data to generate the session The SSL handshake allows the establishment
of a secured connection over an insecure channel. Even if a third party were to listen to the conversation, it would not be able to obtain the session keys. The process of creating good random numbers and applying hash functions can be quite slow, but usually the session keys are cached, so the handshake occurs only on the first connection between the parties.
This process works on top of HTTP, so its portable to any platform that supports it, and is in principle applicable to other protocols as well (Welling 2001, p.334). The process described is part of SSL version2.0, but
version 3.0 is supposed to replace it soon. Another standard, Transport Layer Security (TSL) is still in draft and is supposed to replace SSL in the future.

QUESTION 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 filet 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.

Correct Answer: C
Section: (none)
Explanation

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The RBAC model allows a user to act in a certain predetermined manner based on the role the user holds in the
organization. Users can be assigned certain roles system wide.
Reference: Security + (SYBEX) page 12

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honey pot is a computer that has been designed as a target for computer attacks. The benefit of a honey pot system is that it will draw attackers away from a higher value system or it will allow administrators to gain intelligence about an attack strategy.
Reference: Security + (SYBEX) page 185

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The expansion and contraction that occurs during the normal heating and cooling cycles of your system can cause chips and cards, over time, to inch loose from sockets or slots.

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The method used in these attacks place a piece of software between a server and the user. The software intercepts and then sends the information to the server. The server responds back to the software, thinking it is the legitimate client. The attacking software then sends this information on to the server, etc. The man in the middle software may be recording this information, altering it, or in some other way compromising the security of your system.
Reference: Security + (SYBEX) page 57

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fiber, as a media, is relatively secure because it cannot be easily tapped. It is the strongest to defeat against EMI
and RFI in my opinion.

Reference: Security + (SYBEX) page 147

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hoaxes do have the possibility of causing as much damage as viruses. Many hoaxes instruct the recipient to forward the message to everyone that they know and thus causes network congestion and heavy e-mail activity.
Hoaxes also often instruct the user to delete files on their
computer that may cause their computer or a program to quit functioning.

QUESTION 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 email 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Internet message Access Protocol v4 uses port 143 and TCP for connections. POP3 uses port 110 and TCP for
connections and therefore can be filtered out to decrease unnecessary exposure.
Reference: Security + (SYBEX) page 130

QUESTION 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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A virus is a piece of software designed to infect a computer system. The virus may do nothing more than reside on the computer. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
Reference: Security + (SYBEX) page 76

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The chain of custody is a log of the history of evidence that has been collected. This log should catalog every event from the time the evidence is collected.
Reference: Security + (SYBEX) page 457

QUESTION 26
Data integrity is best achieved using a(n)

A. Asymmetric cipher
B. Digital certificate
C. Message digest
D. Symmetric cipher

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Message Digest Algorithm is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity.
Reference: Security + (SYBEX) page 319

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A user obtaining access to a resource they would not normally be able to access. This is done inadvertently by running a program with SUID (Set User ID) or SGID (Set Group ID) permissions - or by temporarily becoming another user.
Reference: Security + (SYBEX) page 522

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds
with a session key and an encrypted private key. The session is secure after this process.
Reference: Security + (SYBEX) page 365

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

1. 1. 9 Data policy
2. 2. 8 Internet connection
3. 3. 7 personnel
4. 4. 5 software

QUESTION 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 22

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A seems to be the most correct of these answer.
B. is incorrect because IM client are not Trojan Horses, but they can be compromised by Trojan Horses.
C. is incorrect because the answer would make IM secure.
D. All IM messaging system that transverse the Internet uses it as a medium.

QUESTION 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)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The DAC model allows the owner of a resource to establish privileges to the information they own. The DAC model would allow a user to share a file or use a file that someone else has shared. The DAC model establishes
an ACL that identifies the users who have authorized to that information. This allows the owner to grant or revoke access to individuals or group of individuals based on the situation. This model is dynamic in nature and allows information to be shared easily between users.

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Business Continuity Planning is the process of implementing policies, controls, and procedures to counteract the
effects of losses, outages, or failures of critical business processes.
Reference: Security + (SYBEX) page 276

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature at A. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Reference: Security + (SYBEX) page 368

QUESTION 35
Secure MIME (S/MIME) is used for :

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.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature at A. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Reference: Security + (SYBEX) page 368

QUESTION 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 overflow
C. Man in the middle attack
D. Blue Screen of Death
E. SYN flood
F. Spoofing attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Buffer overflow occur when an application receives more data that it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Reference: Security + (SYBEX) page 135

QUESTION 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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FTP has a major flaw. The user ID and password are not encrypted and are subject to packet capture.
Reference: Security + (SYBEX) page 138

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 802.11 standard describes the communication that occurs in wireless local area networks (LANs).The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.
WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such
techniques.
Reference: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION 39
when an application receives more data that it is programmed to accept is called :

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Buffer overflow occur when an application receives more data that it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Reference: Security + (SYBEX) page 135

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IPSec provides secure authentication and encryption of data and headers. IPSec can work in Tunneling mode or
Transport mode. In Tunneling mode, the data or payload and message headers are encrypted. Transport modes
encrypts only the payload.
Reference: Security + (SYBEX) page 127

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NAT effectively hides your network from the world. This makes it much harder to determine what systems exist on the other side of the router. Reference: Security + (SYBEX) page 29

QUESTION 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IM clients can also be compromised by malicious code, Trojan Horse programs, and traditional DOS attacks.

Reference: Security + (SYBEX) page 197

QUESTION 44
Which two of the following are symmetric-key algorithms used for encryption?

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The chain of custody is a log of the history of evidence that has been collected. This log should catalog every event from the time the evidence is collected.
Reference: Security + (SYBEX) page 457

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A DMZ is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. A FTP server is can be used my people from outside of your network and should be placed in the DMZ.
Reference: Security + (SYBEX) page 26

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DOS attacks prevent access to resources by users authorized to use those resources. An attacker may attempt to
bring down an e-commerce website to prevent or deny usage by legitimate customers.
Reference: Security + (SYBEX) page 53

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The goal of confidentiality is to prevent or minimize unauthorized access and disclosure of data and information.
Reference: Security + (SYBEX) page 22

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This means that a process has no more privileges that necessary to be able to fulfill its functions.

QUESTION 51
Documenting change levels and revision information is most useful for:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Disaster recovery is the ability to recover system operations after a disaster. One of the key aspects of disaster recovery planning is designing a comprehensive backup plan. This includes backup storage, procedures and maintenance.
Reference: Security + (SYBEX) page 405

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sniffers can be mitigated using a Switch. The switch is intelligent and sends the data only to the destination address. Sniffers usually work in a LAN using a hub.

QUESTION 53
Notable security organizations often recommend only essential services be provided by a particular host, and any unnecessary services be disabled. 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
B is wrong because the hardware and software are used usually used in a wide array of different vendors.

QUESTION 54
Which of the following backup methods copies only modified files since the last full backup?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A differential backup is similar in function to an incremental backup, but it backs up any files that have been altered since the last full backup.
Reference: Security + (SYBEX) page 413

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Single Loss Expectancy is the cost of a single loss when it occurs.
Reference: Security + (SYBEX) page 470

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Due Care policies identify what level of care is used to maintain the confidentiality of private information. These policies specify how information is to be handled. The objectives of Due Car policies are to protect and safeguard customer and/or client records.
Reference: Security + (SYBEX) page 428

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Here are some of the common standard that use symmetric algorithm.
. • DES
. • AES has replaced DES as the current standard, and it uses the Rijindael algorithm.
. • 3DES
. • CAST
. • RC
. • Blowfish
. • IDEA
Reference: Security + (SYBEX) page 321-322

QUESTION 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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Preservation of evidence requires limited access. Answer A and B are the best choice. Answer C is wrong, because many incidents that occur in a computer system, especially Internet attacks, will only show up in system RAM while the system is running. Answer D is wrong, because you should not touch anything until the authorities arrive.
Reference: Security + (SYBEX) page 456-458

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Penetration testing is the act of gaining access
Reference: Security + (SYBEX) page 521

QUESTION 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Leaving additional network services enabled may cause difficulties and can create vulnerabilities in your network. As much as possible, configure your network devices as restrictively as you can.
Reference: Security + (SYBEX) page 235

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The goal of integrity is the make sure that the data being working with is actually correct data

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The key word is decentralized, so the best answer would be B.
Reference: Security + (SYBEX) page 432

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Wired Equivalent Privacy is a wireless protocol designed to provide privacy equivalent to that of a wired

network.
Reference: Security + (SYBEX) page 372

QUESTION 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 No repudiation Header (NH) for identity integrity.
F. Provides the Encapsulation Security Payload (ESP) for data confidentiality.

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IPSec is a security protocol that provides authentication and encryption across the Internet. IPSec can use AH or
ESP.
Reference: Security + (SYBEX) page 371

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked. This information is published in the CRL and becomes available using OCSP.
Reference: Security + (SYBEX) page 338

QUESTION 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Renaming the administrator account name and disabling the guest account will reduce the risk of a computer being attacked.

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A dictionary attack is an attack which uses a dictionary of common words to attempt to find the password of a user.
Reference: Security + (SYBEX) page 58

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Symmetrical Keys present a difficult challenge to both a key management and a security perspective. The loss or compromise of a symmetrical key compromises the entire system. Single key systems are entirely dependant
on the privacy of the key. This key requires special handling and security. Make sure that symmetrical keys are never divulged. Symmetrical keys should be transmitted using secure out-of band
methods.
Reference: Security + (SYBEX) page 385-386

QUESTION 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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
I disagree with the original answer C. The man in the middle attack can steal the hashed password, and then it can be decrypted at their own leisure.
Reference: Security + (SYBEX) page 57

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The NTFS was introduced with Windows NT to address security problems. With NTFS files, directories, and volumes can each have their own security.
Reference: Security + (SYBEX) page 229

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer B would best benefit the policy for your company to adjust to certain needs for or less depending on the risk. Answer A is wrong because not every threat can be fixed.
Answer C is wrong because it may cost more money to address every risk than what the company makes.
Answer D is obviously wrong.

QUESTION 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. Brute force attack
D. Reverse DNS (Domain Name Service)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 56

QUESTION 74
Active detection IDS systems may perfor m 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Active response involves taking an action based upon an attack or threat. The goal of an active response would be to take the quickest action possible to reduce the potential impact of an event. Terminating connections, processes, or sessions are responses that may occur in the event of a unauthorized connection.
A and C are wrong for obvious reasons.
Reference: Security + (SYBEX) page 181

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honey pot is a computer that has been designed as a target for computer attacks.
Reference: Security + (SYBEX) page 185

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A virus is a piece of software designed to infect a computer system. I can go into this further, but the answer is obvious.
Reference: Security + (SYBEX) page 76

QUESTION 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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A VLAN allows you to create groups of users and systems and segment them on the network. This segmentation allows you to hide segments of the network from other segments and control access. You can think of a VLAN as a good way to contain network traffic. VLANS are created by using a switch and switched networks mitigate against sniffers.
Reference: Security + (SYBEX) page 28

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Access control defines how users and systems communicate and in what manner. Three basic models are used
to explain access control.
Reference: Security + (SYBEX) page 11

QUESTION 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

Correct Answer: H
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The current version of IMAP (IMAP4) uses port 143 and TCP for connection.
Reference: Security + (SYBEX) page 130

QUESTION 80
What is access decisions based on in a MAC (Mandatory Access Control) environment?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 81
As the Security Analyst for your companies network, you want to implement AES ?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AES has replaced DES as the current standard, and it uses the Rijindael
Reference: Security + (SYBEX) page 22

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's email address, and the password was anonymous.
Reference: Security + (SYBEX) page 137

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 322

QUESTION 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The best choices would be B and C. When an incident occurs, the best thing to do is document what is going on
and call the incident response team. By logging off the network, you can damage evidence. If the system is being attacked over the internet, then shutting the system down will corrupt the data and evidence.
Reference: Security + (SYBEX) page 456

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 530

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A virus can do many things and including itself in a program is one of them. A virus is a program intended to damage a computer system.
Reference: Security + (SYBEX) page 533

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions. Most accounting systems and database management systems include an audit trail component. In addition, there
are separate audit trail software products that enable network administrators to monitor use of network resources.

QUESTION 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 is 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 89
DAC (Discretionary Access Control) system operates 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The DAC model allows the owner of a resource to establish privileges to the information they own. The DAC model would allow a user to share a file or use a file that someone else has shared. The DAC model establishes

an ACL that identifies the users who have authorized to that information. This allows the owner to grant or revoke access to individuals or group of individuals based on the situation. This model is dynamic in nature and allows information to be shared easily between users.
Reference: Security + (SYBEX) page 12

QUESTION 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Biometric systems are those that use some kind of unique biological identifier to identify a person. Some of these unique identifiers include fingerprints, patterns on the retina, and handprints, and DNA scanners, and they
can be used as part of the access control mechanisms. Usernames, passwords and PINs are not apart of biometrics.
Reference: Security + (SYBEX) page 265

QUESTION 91
As the Security Analyst for your company's network, you want to implement Single Sign-on technology. What benefit can you expect to get when implementing Single Sign-on?

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The purpose of a single sign-on is so that a user can gain access to all of the applications and systems they need
when they log on.
Reference: Security + (SYBEX) page 434

QUESTION 92
Misuse-Detection IDS is primarily focused on evaluating attacks based on attack_____:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IDS can detect two types of traffic patterns. Misuse-Detection IDS is primarily focused on evaluating attacks based on attack signatures and audit trails. Anomaly-Detection IDS focuses on abnormal traffic patterns.
Reference: Security + (SYBEX) page 177-178

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Multi-Factor When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
Reference: Security + (SYBEX) page 17

QUESTION 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Answer A is correct to stop anyone from corrupting the evidence.
Answer B is incorrect, because you would want the incident response team there.
Answer C is incorrect, because that would corrupt any evidence that is stored in RAM.
Answer D is correct to stop all activity to the hacker.

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You want evidence usable of it is needed for a trial. It is a good idea to seal evidence into a bag and identify the date, time, and person who collected it. This bag-and-tag process makes tampering with the evidence more difficult.
Reference: Security + (SYBEX) page 458

QUESTION 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)
Reference: Standards for Security

Correct Answer:
Section: (none)
Explanation

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: RAID is a technology that uses multiple disks to provide fault tolerance.
Reference: Security + (SYBEX) page 404

QUESTION 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)

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Four popular asymmetric systems are in use today:
. • RSA
. • Diffie-hellman
. • ECC
. • El Gamal
Reference: Security + (SYBEX) page 324

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Secure Sockets Layer (SSL) protocol uses both asymmetric and symmetric key exchange. Use asymmetric
keys for the SSL handshake. During the handshake, the master key, encrypted with the receiver public passes from the client to the server. The client and server make their own session keys using the master key. The session keys encrypt and decrypt data for the remainder of the session. Symmetric key exchange occurs during the exchange of the cipher specification, or encryption level.

QUESTION 100
What would NOT improve the physical security of workstations?

A. Lockable cases, keyboards, and removable media drives.
B. Key or password protected configuration and setup.
C. Password required to boot.
D. Strong passwords.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This is a tough question. The best choice is A, because physical security starts with the entrance and works its way towards the rooms where computers are stored. If by the chance a intruder gets to a workstation, they can still access it even though it is locked.
Reference: Security + (SYBEX) page 258

QUESTION 101
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Certification revocation is the process of revoking a certification before it expires. A certificate may need to be revoked because it was stolen, an employee moved on to a new company, or someone has had their access revoked.
Reference: Security + (SYBEX) page 337

QUESTION 102
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Single Loss Expectancy is the cost of a single loss when it occurs.
Reference: Security + (SYBEX) page 470

QUESTION 103
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You want evidence usable of it is needed for a trial. It is a good idea to seal evidence into a bag and identify the date, time, and person who collected it. This bag-and-tag process makes tampering with the evidence more difficult.
Reference: Security + (SYBEX) page 458

QUESTION 104

Providing false information about the source of an attack is known as:

A. Aliasing
B. Spoofing
C. Flooding
D. Redirecting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A spoofing attack is simple an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack.
Reference: Security + (SYBEX) page 56

QUESTION 105
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Fiber, as a media, is relatively secure because it cannot be easily tapped. It is the strongest to defeat against EMI
and RFI in my opinion.
Reference: Security + (SYBEX) page 147

QUESTION 106
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds

with a session key and an encrypted private key. The session is secure after this process.
Reference: Security + (SYBEX) page 365

QUESTION 107
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 108
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 109
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The key word is decentralized, so the best answer would be B.
Reference: Security + (SYBEX) page 432

QUESTION 110

What is access decisions based on in a MAC (Mandatory Access Control) environment?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 111
DAC (Discretionary Access Control) system operates 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The DAC model allows the owner of a resource to establish privileges to the information they own. The DAC model would allow a user to share a file or use a file that someone else has shared. The DAC model establishes
an ACL that identifies the users who have authorized to that information. This allows the owner to grant or revoke access to individuals or group of individuals based on the situation. This model is dynamic in nature and allows information to be shared easily between users.
Reference: Security + (SYBEX) page 12

QUESTION 112
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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Four popular asymmetric systems are in use today:
. • RSA
. • Diffie-hellman
. • ECC
. • El Gamal

Reference: Security + (SYBEX) page 324

QUESTION 113
prevent or minimize unauthorized access and disclosure of data
and information is:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: The goal of confidentiality is to prevent or minimize unauthorized access and disclosure of data and information.
Reference: Security + (SYBEX) page 22

QUESTION 114
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A honey pot is a computer that has been designed as a target for computer attacks.
Reference: Security + (SYBEX) page 185

QUESTION 115
As the Security Analyst for your companies network, you want to implement AES ?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
AES has replaced DES as the current standard, and it uses the Rijindael
Reference: Security + (SYBEX) page 22

QUESTION 116
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

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, be e-mail, or by a visit.
Reference: Security + (SYBEX) page 87

QUESTION 117
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked. This information is published in the CRL and becomes available using OCSP.
Reference: Security + (SYBEX) page 338

QUESTION 118
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.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page

QUESTION 119
How many bits are employed when using has encryption?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: Security + (SYBEX) page 183

QUESTION 120
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Access control defines how users and systems communicate and in what manner. Three basic models are used
to explain access control.
Reference: Security + (SYBEX) page 11

QUESTION 121
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Multi-Factor When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
Reference: Security + (SYBEX) page 17

QUESTION 122
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

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, be e-mail, or by a visit.
Reference: Security + (SYBEX) page 87