QUIZZ 1

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

19) _____ is defined as "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources". 19) Computer Security

20) An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is an _____ . 20) attack

21) A loss of _____ is the disruption of access to or use of information or an information system. 21) availability

22) A possible danger that might exploit a vulnerability, a _____ is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. 22) threat

23) A _____ attack attempts to learn or make use of information from the system but does not affect system resources. 23) passive

24) Active attacks can be subdivided into four categories: replay, modification of messages, denial of service, and _____ . 24) masquerade

25) X.800 divides security services into five categories: authentication, access control, nonrepudiation, data integrity and _____ . 25) data confidentiality

26) _____ prevents either sender or receiver from denying a transmitted message; when a message is sent the receiver can prove that the alleged sender in fact sent the message and when a message is received the sender can prove that the alleged receiver in fact received the message. 26) Nonrepudiation

27) A _____ is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. 27) digital signature

QUIZ-2

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

16) A _____ cipher processes the plaintext input in fixed sized blocks and produces a block of ciphertext of equal size for each plaintext block.
16) BLOCK

17) With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the _____ .
17) KEY

18) The process of attempting to discover the plaintext or key is known as _____ .
18) CRYPTANALYSIS

19) An encryption scheme is _____ if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.
19) COMPUTATIONALLY SECURE

20) _____ is a stream cipher used in the Secure Sockets Layer/Transport Layer Security standards that have been defined for communication between Web browsers and servers and is also used in WEP and WPA protocols.
20) RC4

21) In the _____ mode the input to the encryption algorithm is the XOR of the current plaintext block and the preceeding ciphertext block; the same key is used for each block.
21) cipher block chaining (CBC)

22) Two requirements for secure use of symmetric encryption are: sender and receiver must have obtained copies of the secret key in a secure fashion and a strong _____ is needed.
22) encryption algorithm

23) All encryption algorithms are based on two general principles: _____, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.
23) substitution

24) Many symmetric block encryption algorithms including DES have a structure first described by _____ of IBM in 1973.
24) Horst Feistel

25) The _____ algorithm takes the ciphertext and the same secret key and produces the original plaintext.
25) decryption

QUIZ-3

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

19) Protection against active attack (falsification of data and transactions) is known as _____ . 19) message authentication

20) The _____ approach has two advantages: it provides a digital signature as well as message authentication and it does not require the distribution of keys to communicating parties. 20) public-key

21) Like the MAC, a _____ accepts a variable size message *M* as input and produces a fixed size message digest H(*M*) as output. Unlike the MAC, it does not take a secret key as input. 21) hash function

22) As with symmetric encryption there are two approaches to attacking a secure hash function: brute-force attack and _____ . 22) cryptanalysis

23) The key algorithmic ingredients of _____ are the AES encryption algorithm, the CTR mode of operation, and the CMAC authentication algorithm. 23) CCM

24) A _____ is when the sender "signs" a message with its private key, which is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message. 24) digital signature

25) Bob uses his own private key to encrypt the message. When Alice receives the ciphertext she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore the entire encrypted message serves as a _____ . 25) digital signature

QUIZ-4

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) The strength of any cryptographic system rests with the _____ technique, a term that refers to the means of delivering a key to two parties that wish to exchange data without allowing others to see the key. 21) key distribution

22) A _____ indicates the length of time for which a ticket is valid (e.g., eight hours). 22) lifetime

23) When two end systems wish to communicate they establish a logical connection and, for the duration of that logical connection, all user data are encrypted with a one-time _____ which is destroyed at the end of the session. 23) session key

24) Rather than building elaborate authentication protocols at each server, _____ provides a centralized authentication server whose function is to authenticate users to servers and servers to users. 24) Kerberos

25) _____ defines a framework for the provision of authentication services by the X.500 directory to its users and defines alternative authentication protocols based on the use of public-key certificates. 25) X.509

QUIZ-5

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) _____ provides security services between Transport Layer Protocol and applications that use TCP.
21) Secure Socket Layer (SSL)

22) The _____ Protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm along with cryptographic keys to be used to protect data sent in an SSL Record.
22) Handshake

23) _____ attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
23) Passive

24) _____ provides confidentiality using symmetric encryption and message integrity using a message authentication code.
24) SSL/TLS

25) The _____ takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.
25) SSl Record Protocol

QUIZ-6

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) _____ specifies security standards for IEEE 802.11 LANs including authentication, data integrity, data confidentiality, and key management.
21) IEEE 802.11i

22) The _____ is a universal open standard developed to provide mobile users of wireless phones and other wireless terminals such as pages and personal digital assistants access to telephony and information services including the Internet and the Web.
22) Wireless Application Protocol (WAP)

23) Derived from the GMK, the _____ is used to provide confidentiality and integrity protection for multicast/broadcast user traffic.
23) Group Temporal Key (GTK)

24) The smallest building block of a wireless LAN is a _____ which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.
24) basic service set (BSS)

25) The WAP Programming Model is based on three elements: the client, the original server, and the _____ .
25) gateway

QUIZ-7

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) The key legitimacy field, the signature trust field and the owner trust field are each contained in a structure referred to as a _____ . — 21) trust flag byte

22) PGP provides compression using the _____ algorithm. — 22) ZIP

23) To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using _____ conversion. — 23) radix-64

24) PGP makes use of four types of keys: public keys, private keys, one-time session keys, and _____ symmetric keys. — 24) passphrase based

25) A specification for cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream, _____ allow message recipients to verify the signature by querying the signer's domain directly to retrieve the appropriate public key and thereby confirming that the message was attested to by a party in possession of the private key for the signing domain. — 25) Domain Keys Identified Mail (DKIM)

QUIZ-8

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) IPsec encompasses three functional areas: authentication, key management, and _____ . — 21) confidentiality

22) _____ mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPsec. — 22) Tunnel

23) IPsec policy is determined primarily by the interaction of two databases: The security policy database and the _____ . — 23) security association database (SAD)

24) Confidentiality is provided by an encryption format known as _____ . — 24) encapsulating security payload

25) A _____ attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. — 25) replay

QUIZ-9

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) _____ detection involves the collection of data relating to the behavior of legitimate users over a period of time. Statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior. 21) Statistical anomaly

22) The three classes of intruders identified by Anderson are: Masquerader, Misfeasor, and _____. 22) Clandestine user

23) Password files can be protected in one of two ways: One-way function or _____. 23) Access control

24) Metrics that are useful for profile-based intrusion detection are: counter, gauge, resource utilization, and _____. 24) interval timer

25) Two types of audit records used are Detection-specific audit records and _____ audit records. 25) Native

QUIZ-10

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) Worms and bot programs are examples of _____ malicious software programs. 21) independent

22) A _____ attack is an attempt to prevent legitimate users of a service from using that service. 22) denial of service (DoS)

23) _____ software is essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. 23) Parasitic

24) The _____ is code embedded in some legitimate program that is set to "explode" when certain conditions are met. Examples of such conditions that can be used as triggers are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application. 24) logic bomb

25) _____ technology enables the antivirus program to easily detect even the most complex polymorphic viruses while maintaining fast scanning speeds. 25) Generic decryption (GD)

QUIZ-11

SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.

21) A _____ forms a barrier through which the traffic going in each direction must pass and dictates which traffic is authorized to pass. 21) firewall

22) The four general techniques that firewalls use to control access and enforce the site's security policy are: service control, direction control, user control, and _____ control. 22) behavior

23) Four types of firewalls are: Packet filtering, stateful inspection, circuit level proxy and _____. application proxy 23) _____

24) A _____ sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established TCP segments from one connection are relayed to the other without examining the contents. 24) circuit level gateway

25) Typically serving as a platform for an application level or circuit level gateway, a _____ is a system identified by the firewall administrator as a critical strong point in the network's security. 25) bastion host