CNS U-1 saqs

1) What is network security?

A) Network security is any activity designed to protect the usability and integrity of your network and data.

->It targets a variety of threats

->It stops them from entering or spreading on your network

2) What is a Security Attack ?

A) An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

3)* What are security services? (LAQ)

A) Authentication , Access control , Data confidentiality , Data integrity , Nonrepudiation , Availibilityservice .

4) Define the terms confidentiality and authentication.

A) -> Confidentiality : is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified.

-> Authentication service is concerned with assuring that a communication is authentic. The function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

5) Differentiate between active attack and passive attack

Active Attack	**Passive Attack**
1. In active attack, Modification in information take place.	While in passive attack, Modification in the information does not take place.
2.Active Attack is danger for Integrity as well as availability.	Passive Attack is danger for confidentiality
3.In active attack attention is on detection.	While in passive attack attention is on prevention.

6) What is Denial of Service?

A) It is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic .

7) What is steganography?

A) It is the practice of hiding a secret message inside of something that is not secret.

-> involves the use of any medium to hide messages

8) What is RFC?

A) -> Request for Comments

-> a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet, along with Internet-connected systems.

CNS UNIT - 2 SAQS

1) What is cryptography?

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents

2) What are the dimensions used for classifying cryptographic algorithms?

1. The type of operations used for transforming plaintext to ciphertext.
2. The number of keys used.
3. The way in which the plaintext is processed.

3) What is the difference between a block cipher and a stream cipher?

Block ciphers process messages in blocks, each of which is then en/decrypted.
Stream ciphers process messages a bit or byte at a time when en/decrypting.

4) What are the essential ingredients of symmetric cipher?

There are five main components of a symmetric encryption system: plaintext, encryption algorithm, secret key, ciphertext, and the decryption algorithm.

5) What are the design parameters of Feistel cipher network?

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis

6) How many rounds are there in DES algorithm?

The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

7) What are the strengths of DES?

- The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on such number of keys is impractical.
- The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

8) What are block cipher modes of operation?

There are five types of operations in block cipher modes, ECB (Electronic Code Block) mode, CBC (Cipher Block Chaining) mode, CFB (Cipher Feedback) mode, OFB (Output Feedback) mode and CTR (Counter) mode.

9. What are the advantages and disadvantages of Electronic Code Book mode?

Advantages of using ECB :

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB :

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

10. What are the different approaches for attacking a cipher?

Cryptanalysis , Brute-force attack

11. What is digital signature?

The sender —signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

12. What is the difference between link and end-to-end encryption?

Link Encryption	End-to-End Encryption
1)Message exposed in sending host	1)Message encrypted in sending host
2)Message exposed in intermediate nodes	2)Message encrypted in intermediate nodes
3)Provides host authentication	3)Provides user authentication

13. Define weak collision property of a hash function.

Weak collision resistance (CR), or second-preimage resistance, is the property that given x and h(x) (h a hash function) it's difficult to find $x' \neq x$ such that $h(x')=h(x)$.

14. Differentiate between MAC and hash function.

A cryptographic **hash function** takes as input a sequence of bits and outputs values in a rather small space, typically a sequence of bits with a fixed size.

A **message authentication code(MAC)** is an algorithm which takes as input a message and a secret key and produces a fixed-sized output which can be later on verified to match the message; the verification also requires the same secret key.

15. What is the basic idea behind HMAC?

Hash-based message authentication code (or HMAC) is a cryptographic technique that combines public keys, private keys, and a hash into a mix hackers can't unpack. Use HMAC, and you'll tap into a method that can both encrypt data and check the integrity of information you get in return.

16. What is Key Distribution Center?

A key distribution center (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data. Each time a connection is established between two computers in a network, they both request the KDC to generate a unique password which can be used by the end system users for verification.

17. What is MD5?

The MD5 (message-digest algorithm) hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

18. What are the differences between Symmetric and Asymmetric cryptography?

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is slow.	The encryption process is very fast.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.

19. What are the keys involved in public-key cryptography?

- Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key.
- Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key.

20. Which key is used for digital signature?

Digital signature transaction includes a pair of keys: a private key and a public key.

- Public key– Key which is known to everyone.
- Private key– Key which is only known to the person who’s private key it is.

21. Who provides digital certificates?

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant’s public key and a variety of other identification information

22. What are the applications of public-key cryptography?

1. Encryption/Decryption
2. Digital signature
3. Key exchange

CNS U-3 saqs

1) What is Kerberos?

A) -> it is an authentication service developed as part of Project Athena at MIT.

-> provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

2) What is IDC in Kerberos?

A) identifier of user on C (client) .

3) Who issues the tickets to users who have been authenticated to AS?

A) Kerberos .

6) What is X.509 service?

A) it includes three alternative authentication procedures that are intended for use across a variety of applications.

7) Define forward certificates.

A) Certificates of X generated by other CA (certification authority)

8) Define reverse certificates.

A) Certificates generated by X that are the certificates of other CA .

9) What is one-way authentication?

A) -> involves a single transfer of information from one user (A) to another (B)

-> establishes the following:

->identity of A and that the message was generated by A

->the message was intended for B

-> integrity and originality of the message

10) What is two-way authentication?

A) -> permits both parties in a communication to verify the identity of the other.

->establishes the following elements:

-> identity of B and that the reply message was generated by B

->message was intended for A

-> integrity and originality of the reply

11) .What is three-way authentication?

A) a final message from A to B is included, which contains a signed copy of the nonce rB

13)* What are the services provided by PGP?

A) LAQ answer

14) What are the notations in PGP, Ks, KRa, KUa, EC, DC?

A) Ks =session key used in symmetric encryption scheme

PRa =private key of user A, used in public-key encryption scheme

PUa =public key of user A, used in public-key encryption scheme

EP = public-key encryption

DP = public-key decryption

EC = symmetric encryption

DC = symmetric decryption

H = hash function

15) How digital signature is generated?

A) -> are created and verified by using public key cryptography, also known as asymmetric cryptography.

-> By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.

(few answers as part of IMPortant laqs have not been written here - all PGP services individually)

23) What is time stamp?

A) Time at which signature is made .

24) What is message digest?

A) -> 160-bit SHA-1 digest, encrypted with the sender's private signature key.

-> It is calculated over the signature timestamp concatenated with the data portion of the message component.

25) What is private key ring?

A) -> is a table of rows containing: Timestamp ; Key ID ; Public key ; Private key ; User ID

26) What is public key ring?

A) -> is used to store public keys of other users that are known to this user .

-> it has :-

key legitimacy field ; signature trust field ; owner trust field .

27) . What is multipart type?

A) -> indicates that the body contains multiple, independent parts.

-> 4 "subtypes"

multipart/mixed ; multipart/parallel ; multipart/alternative ; multipart/digest

28) What is message/partial subtype?

A) enables fragmentation of a large message into a number of parts, which must be reassembled at the destination.

29) What is enveloped data?

A) consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.

30) Signed data :

A) -> A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer.

-> A signed data message can only be viewed by a recipient with S/MIME capability.

31) What is registration in S/MIME?

A) user's public key must be registered with a certification authority in order to receive an X.509 public-key certificate.

32) What is secure mailing list?

A) It uses MLA (mail list agent) that can take a single incoming message, perform the recipient-specific encryption for each recipient, and forward the message .

U-4 saqs :

1) Write two applications of IP Security.

A) Secure branch office connectivity over the Internet ; Secure remote access over the Internet

2) Write two benefits of IP Security .

A) -> it provides strong security that can be applied to all traffic crossing the perimeter.

-> it is transparent to end users .

3) What are the IP security services?

A) Access control ; Connectionless integrity ; Data origin authentication ; Confidentiality ; Limited traffic flow confidentiality

4) What is SPI?

A) The SPI (Security Parameters Index) is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

5) What is anti replay window?

A) Used to determine whether an inbound AH or ESP packet is a replay .

7)* What is transport mode?

A) -> It provides protection primarily for upper-layer protocols.

-> transport mode protection extends to the payload of an IP packet.

8) What is tunnel mode?

A) -> provides protection to the entire IP packet.

-> To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header.

9) What is replay attack?

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

10) What is integrity check value?

A) is a message authentication code produced by a MAC algorithm.

12)* What are the fields in ESP format?

A) Security Parameters Index ; Sequence Number ; Payload Data ; Padding ; Pad Length ; Next Header ; Authentication Data

13)* What is virtual private network?

A) -> It is an encrypted connection over the Internet from a device to a network.

->The encrypted connection helps ensure that sensitive data is safely transmitted.

14) What is security association bundle?

A) refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services.

16)* Write the two types of key management .

A) -> Manual: A system administrator manually configures each system with its own keys and with the keys of other communicating systems.

-> Automated: An automated system enables the on-demand creation of keys for SAs .

17) Define cookie exchange .

A) requires that each side send a pseudorandom number, the cookie, in the initial message, which the other side acknowledges.

18)* Proposal payload :

A) -> It contains information used during SA negotiation.

->The payload indicates the protocol for this SA (ESP or AH) for which services and mechanisms are being negotiated.

19)* Transform payload :

A) -> It defines a security transform to be used to secure the communications channel for the designated protocol.

-> # parameter serves to identify this particular payload so that the responder may use it to indicate acceptance of this transform .

20)* Certificate payload :

A) It transfers a public-key certificate. The Certificate Encoding field indicates the type of certificate or certificate-related information

21)* Hash payload :

A) -> contains data generated by a hash function over some part of the message and/or ISAKMP state.

-> may be used to verify the integrity of the data in a message or to authenticate negotiating entities.

22)* Nonce payload :

A) contains random data used to guarantee liveness during an exchange and protect against replay attacks.

23) What are the web security threats?

A) Phishing

Ransomware

SQL injection

Cross-site scripting

Code injection

Viruses and worms

Spyware

24) What is SSL?

A) -> known as Secure Socket Layer .

-> designed to make use of TCP to provide a reliable end-to-end secure service.

-> it is 2 layers of protocols (tcp , ip)

25) What is master secret?

A) 48-byte secret shared between the client and server.

26) What is sequence number?

A) 32 bit monotonically increasing counter value that provides an anti-replay function.

27) What is message integrity?

A) defines a shared secret key that is used to form a message authentication code (MAC) .

29) What is alert protocol?

A) used to convey SSL-related alerts to the peer entity .

30)* What is handshake protocol?

A) -> most complex part of SSL is the Handshake Protocol.

-> allows the server and client to authenticate each other and to negotiate an encryption to protect data sent in an SSL record.

33) What is no renegotiation?

A) -> Sent by a client in response to a hello request or by the server in response to a client hello after initial handshaking.

Either of these messages would normally result in renegotiation, but this alert indicates that the sender is not able to renegotiate.

35) What is merchant authentication?

A) SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards .

36) What is integrity of data in SET?

A) -> Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions.

->SET guarantees that these message contents are not altered in transit.

37)* What is the purpose of dual signature in SET protocol?

A) -> links two messages that are intended for two different recipients : - the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank .

-> guarantees the authentication and integrity of data.

38)* What is payment gateway?

A) -> it is the technology that captures and transfers payment data from the customer to the acquirer.

-> keeps the payments ecosystem rolling smoothly .

-> The merchant exchanges SET messages with the payment gateway over the Internet .

39) What is initial response?

A) ->It is an organized approach to address and manage the aftermath of a security breach or cyberattack .

-> it limits damage and reduces recovery time and costs.

40) What is capture reversal?

A) Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.

41)* What is card holder certificate?

A) It contains the cardholder's public signature key. It is needed by the merchant and by the payment gateway.

U-5 saqs :

2) What are the components of SNMP?

A) SNMP Manager ; SNMP agent ; Management Information Base

3) What is Management Agent?

A) It is a software process that responds to SNMP queries to provide status and statistics about a network node.

4) What is Management Information Base?

A)-> Information about the target device is contained in a Management Information Base (MIB).

-> It tells about the device's functions and data.

5)* What is SNMP?

A) -> It is an Internet Standard protocol used to monitor and manage the network devices connected over an IP.

-> It collects data from these devices, organizes them, and sends them for network monitoring and management with fault detection and isolation.

-> It serves as an integral part of both the monitored endpoints and the monitoring system.

6) What are proxies ?

A) -> It is a server that translates traffic between networks or protocols.

-> It’s an intermediary server separating end-user clients from the destinations that they browse.

7) What is SNMP community?

A) It is a type of shared password between the SNMP management station and the device, which is used to authenticate the SNMP management station.

8)What is access policy?

A) -> They are a list of roles and the resources with which roles are to be provisioned or deprovisioned.

-> It is used to automate the provisioning of target systems to users.

10) What is proxy service ?

A) A proxy service is an intermediary role played by software or a dedicated computer system between an endpoint device and a client which is requesting the service.

11)What is traditional SNMP manager ?

A) ->It is a centralized system used to monitor network.

-> It is also known as Network Management Station (NMS) .

12) What is SNMP agent ?

A) -> An SNMP agent is a software process that responds to SNMP queries to provide status and statistics about a network node.

-> SNMP agents play the most important role in management.

-> They are locally located and associated with SNMP network devices from which they collect, store, and transmit monitoring data.

13)Which application makes use of the send PDU and process Response PDU dispatcher primitives?

A) Command generator application

14) What is command responder application?

A) -> It is a general purpose, cross-platform, extendable and multi-protocol SNMP agent implementation.

-> It exposes interesting traits of a system being managed through SNMP

16)What is masquerade?

A) It a process where one computer acts as an IP gateway for a network. All computers on the network send their IP packets through the gateway, which replaces the source IP address with its own address and then forwards it to the internet .

17) What is disclosure?

A) It is when a website unintentionally reveals sensitive information to its users .

18)* What is denial of service?

A) -> It is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

-> DoS attacks accomplish this by flooding the target with traffic .

20) What is MIB context?

A) It is a context–based access feature provides ability to query the Interfaces MIB objects and the information returned will be restricted to the VRF (virtual route forwarding) .

21)* What is misfeasor?

A) A legitimate user who accesses data, programs, or resources for which such access is not authorized but misuses his or her privileges.

22) What is one-way encryption?

A) It is a type of encryption and can be used to securely store data for retrieval at a later date with the use of a password and another function.

23)* What is proactive password checker?

A) It is a program that interacts with the user when he tries to change his own password. The proposed password is checked and the change is allowed only if it is hard-to-guess.

24)* What is intrusion detection?

A) -> It is monitoring of network traffic for suspicious activity and issues alerts when such activity is discovered.

-> It is a software application that scans a network or a system for harmful activity or policy breaching.

25)* What is rule based detection?

A) ->it is searching for patterns linked to specific types of attacks .

-> has established patterns that do not change with new data .

26) What is trap door and logic bomb?

A) Trap door :- secret entry point into a program that allows anyone gain access to any system without going through the usual security access procedures.

Logic bomb :- a malicious program that is triggered when a logical condition is met .

27) What is Trojan horse?

A) a type of malware that downloads onto a computer disguised as a legitimate program.

29) What is virus signature scanner?

A) It uses signatures to track down Trojans, spyware and other software circulated by criminals .

30)* What are various anti-virus techniques?

A) Generic Decryption ; Digital Immune System ; Behavior-Blocking Software .

31)* What is a firewall?

A) -> A firewall forms a barrier through which the traffic going in each direction must pass.

-> effective means of protecting a local system or network of systems from network based security threats .

32) What is packet filtering router?

A) It applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both

directions .

33)* What is IP address spoofing?

A) -> type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity .

-> a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source .

35) What is application-level gateway?

A) -> also called a proxy server, acts as a relay of application-level traffic .

-> tend to be more secure than packet filters.

36) What is circuit level gateway?

A) -> can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications.

-> does not permit an end-to-end TCP connection .

38) What is access matrix?

A) -> is a security model of protection state in computer system .

-> defines the rights of each process executing in the domain with respect to each object.

41) What is trusted system?

A) It is a technology to enhance the ability of a system to defend against intruders and malicious programs .

-> it is commonly found in the military, where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS) .

43) What is IDS?

A) -> Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

-> It is a software application that scans a network or a system for harmful activity or policy breaching.

44)* Name few IDS techniques .

A) Statistical anomaly detection ; Rule-based detection ; Statistical Anomaly Detection

45) What is verifiability?

A) indicates that :

-> The reference monitor's correctness must be provable.

-> it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation.

47) What are capability tickets?

A) It's a process that shows what objects are allowed to access and what operations are allowed on it .

48) What are tiny fragment attacks?

A) -> occurs when a tiny packet fragment gets into the server.

-> This happens when one of the fragments are so small that it can't even fit its own header , can cause reassembly problems and shut down a server.

49) What is bastion host?

A) a special-purpose server or an instance that is used to configure to work against the attacks or threats & acts as aproxy server .

50) What is difference between Host based IDS and Network based IDS?

A) The host-based intrusion detection system can detect internal changes , while a network-based IDS will detect malicious packets as they enter your network .