CSS VIVA QUESTIONS

1. Cryptography:
    - It is the study of secure communications techniques which allows only the sender and the intended receiver to see and read the content of messages, through the uses of codes.

2. Steganography:
    - It is the practice of concealing a message within another message or a physical object.

3. Encryption:
    - Process in which original information/message is transformed into an unrecognizable form.

4. Decryption:
    - Process in which encrypted text is transformed into its original form which is understandable.

5. Plaintext/Cleartext:
    - The decrypted message is returned to its original form/ state of context which is comprehensible.

6. Ciphertext:
    - When a message is encrypted into an unrecognizable state.

7. Security Goals:
    - Confidentiality: data must be kept private, confidential whether it is stored or during transmission.
    - Integrity: changes in data must be only done by authenticated, authorized persons and only secured mechanisms.
    - Availability: information must be available when needed.

8. Types of attacks:
    - Passive: an attacker can only see the data but cannot modify it.
    - Active: an attacker can modify the data and it will cause damages to the victims.

9. Types of security attacks:
    a. Confidentiality attack:
        - Snooping: unauthorized access of data.
        - Traffic Analysis: examining and intercepting messages in order to deduce information by looking from patterns in communication.
    b. Integrity attacks:
        - Modification: modification, changes made in data.
        - Masquerading/Spoofing: when an attacker impersonates somebody to gain information.
        - Replaying: attacker obtains a message of the victim and tries to replay it later.

- Repudiation: when the user denies the fact that he or she has performed a certain action or has initiated a transaction.

c. Availability:
   - Denial of Service (dos): attacker uses many strategies and aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. He achieves this by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to users.
   - Types of Dos Attacks: flood attack, ping of death, SYN attack.

10. Ddos and Dos attacks:
    a. DOS:
       - A DOS attack is a denial-of-service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down.
    b. DDOS:
       - DDOS attack means distributed denial of service in this attack DOS attacks are done from many different locations using many systems.

    c. Difference DOD and DDOS:
       - In DOS attacks, a single system targets the victim's system.
       - In DDOS multiple systems attack the victim's system.

11. Digital Signature:
    - Used to validate the authenticity and integrity of a message, software or digital document.
    - Digital equivalent of a handwritten signature or stamped seal.
    - Offers security.
    - Digital Signature Algorithm is used for processing digital signatures.
    - Digital Signature Schemes – RSA, ELGamal and Schnorr signature schemes.

12. Playfair Cipher:
    - It is a digraph substitution cipher.
    - Uses 5*5 marine table to store the letters of the phrases given for encryption.
    - It encrypts a digraph (pair of 2 letters).

13. Transposition Cipher:
    - Method of encryption in which the positions of the message or plaintext are shifted according to a specific pattern, system.
    - Rail fence and columnar transposition are examples of this type of cipher.

14. Caesar Cipher:
    - Type of substitution cipher.
    - Each letter of the text or the written message is substituted with another letter of the alphabet, forming the ciphertext.

15. Monoalphabetic Ciphers:
    - Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process.
    - For example, if 'A' is encrypted as 'D', for any number of occurrences in that plaintext, 'A' will always get encrypted to 'D'.

16. Polyalphabetic Cipher:
    - Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
    - Playfair and Vigenère Cipher are polyalphabetic ciphers.

17. Vigenere Cipher:
    - It is a form of polyalphabetic cipher.
    - The encryption of the original text is done using the *Vigenère square or Vigenère table*.

    Relationship between vigenere cipher and caesar cipher
    - In a Caesar cipher, each letter of the alphabet is shifted along some number of places. For example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher has several Caesar ciphers in sequence with different shift values.

18. Data Encryption Standard Algorithm (DES):
    - It is a symmetric-key block cipher.
    - It takes the plain text in blocks of 64 bit and converts them into 64-bit ciphertext using a key of 56 bits.
    - There are a total of eight S-box tables.
    - The same key is used for encryption and decryption.
    - It is an implementation of Feistel Cipher, it uses 16 round Feistel Structure.
    - It is one of the mathematical algorithms used in Symmetric Cryptography.

19. Double Data Encryption Standard Algorithm and Triple Data Encryption Standard Algorithm:
    - It is similar to DES but Double Data Encryption Standard Algorithm uses two instances of DES and uses two different keys whereas Triple Data Encryption Standard Algorithm uses three instances of DES and uses three different types of keys.

20. Advanced Encryption Standard Algorithm:
    - It is a symmetric key symmetric block cipher.
    - Input is 128-bit data, keys might be 128/192/256-bit.
    - The number of rounds is variable and depends on the length of the key.
    - The rounds have 4 subprocesses: (1) Byte Substitution, (2) Shift Rows, (3) Mix Columns, (4) Add Roundkey.
    - Stronger and faster than Triple-DES.
    -

21. ElGamal Algorithm:
    - It is a public-key encryption algorithm.
    - It uses asymmetric key encryption for communicating between two parties and encrypting the message.
    - The security of this algorithm depends on the difficulty of computing discrete logs in a large prime modulus.

22. Diffie Hellman Key Exchange Algorithm:
    - Also known as Key Exchange Algorithm or Key Agreement.
    - Used to generate the same private cryptographic key sender as well as receiver end so that there is no need to transfer it from sender to receiver.

23. Mathematical algorithms used in asymmetric cryptography:
    - RSA Algorithm
    - The Diffie-Hellman algorithm
    - The Elliptical Wave Theory algorithm

24. Mathematical algorithms used in symmetric cryptography:
    - The Needham-Schroder algorithm
    - The Digital Encryption Standard algorithm (DES) and The Triple-Digit Encryption Standard algorithm (3DES)
    - The Advanced Encryption Standard algorithm (AES)

25. Symmetric Key System:
    - Uses only the private key for encryption and decryption.
    - The key must be kept private.

26. Asymmetric Key System:
    - Uses public key for encryption and private key for decryption.
    - The public key can be shared but the private key must be kept private.

27. Private Key:
    - Used to both encrypt and decrypt the data.
    - Shared between sender and intended receiver of the data.
    - The private key mechanism is called symmetric being a single key between two parties.

28. Public Key:
    - Only used to encrypt data and a private key with it is used to decrypt the data.
    - Can be used by anyone.
    - The public key mechanism is called asymmetric being two different keys for different purposes.

29. Key Distribution Center:
    - It is a database of all end-users and their respective passwords as well as other trusted servers and computers.

- When an end-user wants to communicate with another end user, he enters his password in the KDC using Kerberos. Once the password is received by KDC, Kerberos then adds the receiving user's information and converts it into a cryptographic key, through a mathematical algorithm.
- Once the encrypted key has been established, the Kerberos then establishes other keys for the encryption of the communication between the sender and the receiver. Those keys are called as tickets which will actually expire at a predetermined time, preventing unauthorized use.

30. Kerberos:
    - Kerberos is an authentication service designed for use in a distributed environment.
    - Kerberos provides a trusted third-party authentication service that enables clients and servers to establish authenticated communication.
    - Computer network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network.
    - Uses the concepts of tickets as tokens to prove the identity of the user.
    - Kerberos is still the best security access protocol available today.

31. Hash Function:
    - It is a one-way mathematical function.
    - Used to encode data but it can't decode data.
    - Its primary purpose is to prove that the message in cipher text has not changed in any way, shape or form.
    - It is referred to as message integrity.

32. Secure Hash Function (SHA-1):
    - It is a hash function.
    - It takes input messages of length less than 2^64 bits and produces an output message of 160 bit.
    - Stronger against Brute Force Attack.
    - It uses four types of rounds, each iterated 20 times for a total of 80 rounds.

33. MD-5:
    - MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value.
    - It takes 4 rounds.

34. Digital Certificate:
    - Used to verify the identity of the certificate holder and issued by the Certificate Authority.
    - Issued to people as well as to computers, software packages or anything else that needs to prove the identity in the electronic world.
    - Allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI).
    - Also known as a public key certificate or identity certificate.

35. Public Key Infrastructure (PKI):
    - It provides assurance of public keys.
    - Its main purpose of PKI is to create, organize, store, distribute and maintain the public keys.

36. Pretty Good Privacy (PGP):
    - Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication.
    - It is an encryption system used for both sending encrypted emails and encrypting sensitive files.
    - PGP encryption uses a combination of two forms of encryption: symmetric key encryption, and public-key encryption.
    - It also provides authentication through Digital Signature.

37. Honeypot:
    - It is a computer or computer system used as a trap for cyber attacks.
    - It can be used to detect attacks and study their types and their tricks.
    - It can also be used to gain information about how cybercriminals operate.
    - Mostly used by large companies involved in cybersecurity.
    - Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

38. Firewall:
    - Barrier between a private internal network and the public Internet.
    - Used to protect any organization from inside-outside hackers.

    How to make a firewall?
    - Collect all the data and ip addresses
    - Design your architecture for the firewall
    - Configure the access control
    - Configure all other firewall services
    - And test your firewall condition

39. Proxy Server:
    - Computer system or router that functions as a relay between client and server.
    - It helps prevent an attacker from invading a private network.
    - It is one of several tools used to build a firewall.

40. Session Hijacking:
    - It is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system.
    - Also known as cookie hijacking.

41. Intrusion Detection System:
    - It is a device or software application that monitors a network or systems for malicious activity or policy violations.
    - It detects different attacks.

- Any intrusion activity is typically reported either to an administrator or collected centrally using a security information and event management system.

42. SQL injection:
    - SQL injection is a code injection technique that might destroy databases.
    - It is one of the most common web hacking techniques.
    - It is the placement of malicious code in SQL statements, via web page input.
    - SQL injection is a server-side attack first and foremost.
    - SQL injection attacks occur when a web application does not validate values received from a web form, cookie, input parameter, etc., before passing them to SQL queries that will be executed on a database server.

43. Traceroute:
    - It is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between.

44. Whois:
    - It is a command used to find out information about a domain, such as the owner of the domain, the owner's contact information, and the nameservers that the domain is using.

45. IPsec:
    - Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
    - It is used in virtual private networks.

46. SSL:
    - Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP.

47. Brute-force attack:
    - The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained.

48. Packet Sniffing:
    - The act of capturing data packets across a computer network is called Packet Sniffing.

49. ARP spoofing:
    - ARP spoofing is a type of attack in which a malicious attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network.
    - This results in the linking of the attacker’s MAC address with the IP address of a legitimate computer or server on the network.
    - Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

50. Port scanning:
    - The act of systematically scanning a computer's ports.
    - Since a port is a place where information goes in and out of a computer, port scanning identifies open doors to a computer.

51. IP spoofing:
    - IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.

52. TCP syn flood:
    - TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

53. DNS Spoofing:
    - Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

54. Steganography:
    - It is the practice of concealing a message within another message or a physical object.

55. Malwares:
    a. Viruses:
        - Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
    b. Worms:
        - A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
    c. Trojans:
        - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms
    d. Logic Bomb:
        - A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
    e. Bots:
        - Program activated on an infected machine that is activated to launch attacks on other machines.
    f. Rootkits:
        - Set of hacker tools used after an attacker has broken into a computer system and gained root-level access.

56. Software Vulnerabilities:
    a. Buffer Overflow:
        - A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.
    b. Cross-site scripting:
        - Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
        - XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.
    c. SQL injection:
        - SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

57. Block Cipher Modes of operations:
    a. Electronic Codebook (ECB):
        - Each block of 64 plaintext bits is encoded independently using the same key.
    b. Cipher Block Chaining (CBC):
        - The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.
    c. Cipher Feedback (CFB):
        - preceding ciphertext is used as input to the encryption algorithm to produce pseudo random output, which is XORed with plaintext to produce the next unit of ciphertext.
    d. Output Feedback (OFB):
        - Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.
    e. Counter (CTR):
        - Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.