TOP 30 Cybersecurity Interview Questions [For Freshers]

1. What is CIA Triad's?

   The **CIA Triad** is a foundational model in cybersecurity, standing for **Confidentiality, Integrity, and Availability**. It outlines the three essential principles that ensure the protection of data and systems.

   a. Confidentiality: - Refers to protecting sensitive information from unauthorized access or disclosure.

   b. Integrity: - Refers to maintaining the accuracy and consistency of data and ensuring that is not tempered with or modified in an unauthorized manner.

   c. Availability: - Refers to ensuring that systems, data and resources are available and accessible to authorized users when needed.

2. What is AAA?

   It is stands for **Authentication, Authorization, and Accounting**. It is a framework for controlling access to resources, ensuring proper identity verification, and tracking the use of system resources.

   a. Authentication: - The process of verifying the identify a user, device, or system attempting a access a network or resources.
   b. Authorization: - The process of granting access to specific resources or information based on user's identity, role, or privileges.
   c. Accounting: - This refers to tracking and recording the actions performed by a user or system. It helps monitor activities, create logs, and maintain an audit trail for future analysis or compliance purposes.

3. What is difference between stateful and stateless firewall?

Parameters	Stateful	Stateless
Philosophy	Stateful firewalls maintain context about active sessions and use "state information" to speed packets processing	Treats each packet in isolation and does not relates to connection state.
Filtering decision	Based on flows and connection state (analyses packet sequences).	Based solely on information in packet headers (IP address, port number, etc
Memory and CPU intensive	High (requires resources to maintain state information for each connection).	Low (does not track connections, so uses fewer resources).
Security	High (tracks connection state, providing deeper inspection).	Low (does not track connection state, making it easier to bypass security)
Connection Status	Known (tracks the state of the connection).	Unknown (each packet is treated independently).
Performance	Slower (due to the overhead of tracking connection states).	Faster (since it doesn't track state or maintain connection information).
Related terms	State information, pattern matching etc.	Header info, IP address, port no etc.

4. Explain DDOS attack and how to mitigate it?
   This again is an important Cybersecurity Interview Question. A DDOS (Distributed Denial of Service) attack is a cyberattack that causes the servers to refuse to provide services to genuine clients. DDOS attack can be classified into two types:

   1. Flooding attacks: In this type, the hacker sends a huge amount of traffic to the server which the server cannot handle. And hence, the server stops functioning. This type of attack is usually executed by using automated programs that continuously send packets to the server.
   2. Crash attacks: In this type, the hackers exploit a bug on the server resulting in the system to crash and hence the server is not able to provide service to the clients.

   You can prevent DDOS attacks by using the following practices:

   - Use Anti-DDOS services
   - Configure Firewalls and Routers
   - Use Front-End Hardware
   - Use Load Balancing
   - Handle Spikes in Traffic

5. Differentiate between Vulnerability Assessment and Penetration Testing?
   Vulnerability Assessment is the process of finding flaws on the target. Here, the organization knows that their system/network has flaws or weaknesses and want to find these flaws and prioritize the flaws for fixing.

   Penetration Testing is the process of finding vulnerabilities on the target. In this case, the organization would have set up all the security measures they could think of and would want to test if there is any other way that their system/network can be hacked.

6. What are the common types of cyber security attacks?

Phishing: Attackers send fraudulent emails or messages that appear to come from reputable sources, aiming to trick users into revealing sensitive information like passwords or financial details.

Malware: Malicious software, including viruses, ransomware, worms, and spyware, designed to damage or exploit systems. Ransomware, for example, encrypts data and demands payment for its release.

Man-in-the-Middle (MitM) Attacks: Attackers intercept communication between two parties to steal data, credentials, or insert malicious content. This often happens on unsecured or public Wi-Fi networks.

Denial of Service (DoS) / Distributed Denial of Service (DDoS): Attackers flood a system or network with excessive traffic, overwhelming it and causing legitimate requests to be denied.

SQL Injection: Attackers insert malicious SQL code into a web application's database query, allowing them to manipulate or gain unauthorized access to the database.

Cross-Site Scripting (XSS): Attackers inject malicious scripts into trusted websites, which then execute in the victim's browser, potentially leading to session hijacking or data theft.

Password Attacks: These include brute force, dictionary attacks, and credential stuffing, where attackers attempt to guess or crack passwords to gain unauthorized access to systems.

Insider Threats: Malicious or careless employees, contractors, or business partners who have access to sensitive information and misuse or expose it.

Zero-Day Exploits: Attacks that target vulnerabilities in software that are unknown to the software vendor and have no available patches.

Advanced Persistent Threats (APTs): Long-term targeted attacks, often by nation-states or well-funded attackers, designed to steal sensitive information or disrupt operations.

7. What is difference between hashing and encryption?
   Both Encryption and Hashing are used to convert readable data into an unreadable format. The difference is that the encrypted data can be converted back to original data by the process of decryption but the hashed data cannot be converted back to original data.

8. What are the different layers of the OSI model?
   An OSI model is a reference model for how applications communicate over a network. The purpose of an OSI reference is to guide vendors and developers so the digital communication products and software programs can interoperate.

   Following are the OSI layers:
   Physical Layer: Responsible for transmission of digital data from sender to receiver through the communication media,
   Data Link Layer: Handles the movement of data to and from the physical link. It is also responsible for encoding and decoding of data bits.
   Network Layer: Responsible for packet forwarding and providing routing paths for network communication.
   Transport Layer: Responsible for end-to-end communication over the network. It splits the data from the above layer and passes it to the Network Layer and then ensures that all the data has successfully reached at the receiver’s end.

   Session Layer: Controls connection between the sender and the receiver. It is responsible for starting, ending, and managing the session and establishing, maintaining and synchronizing interaction between the sender and the receiver.

   Presentation Layer: It deals with presenting the data in a proper format and data structure instead of sending raw datagrams or packets.

   Application Layer: It provides an interface between the application and the network. It focuses on process-to-process communication and provides a communication interface.

9. What is TCP 3-way Handshake?
   A three-way handshake is a method used in a TCP/IP network to create a connection between a host and a client. It's called a three-way handshake because it is a three-step method in which the client and server exchanges packets.

   The three steps are as follows:
   1. The client sends a SYN(Synchronize) packet to the server check if the server is up or has open ports
   2. The server sends SYN-ACK packet to the client if it has open ports
   3. The client acknowledges this and sends an ACK(Acknowledgment) packet back to the server

10. What's the difference between a white box test and a black box test?
    White Box Testing: Testers have full knowledge of the internal structure, design, and implementation of the software or system. This includes access to source code, architecture, and algorithms.

    Black Box Testing: Testers have no knowledge of the internal workings. They evaluate the system solely based on its inputs and outputs without understanding the underlying code or architecture.

11. What is the difference between Vulnerability, Risk and Threat?
    Vulnerability: A weakness in a system (e.g., unpatched software).
    Risk: The potential for loss associated with exploiting a vulnerability (e.g., data breach risk).
    Threat: The potential danger that could exploit a vulnerability (e.g., cybercriminals).

12. What are HIDS and NIDS?
    HIDS (Host IDS) and NIDS (Network IDS) are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions. The only difference is that the HIDS is set up on a particular host/device. It monitors the traffic of a particular device and suspicious system activities. On the other hand, NIDS is set up on a network. It monitors traffic of all device of the network.

13. What is Indicator of Compromise?
    An Indicator of Compromise (IoC) is a piece of evidence or data that suggests a security breach or malicious activity has occurred in a system or network. IoCs are like digital breadcrumbs left behind by attackers that can help cybersecurity teams identify, detect, and respond to potential threats or ongoing attacks.

14. What are OWASP Top 10 Vulnerabilities?
    The **OWASP Top 10** is a list of the most critical web application security risks, compiled by the **Open Web Application Security Project (OWASP)**. It provides guidance to developers, security teams, and organizations on addressing the most common and impactful vulnerabilities. The most recent OWASP Top 10 list (2021) includes the following:
    1. Broken Access Control:
    - **Description**: Flaws that allow users to act outside their intended permissions, such as gaining unauthorized access to restricted resources.

- **Example**: A normal user modifying a URL to access an admin page.

2. Cryptographic Failures:

- **Description**: Weak or improperly implemented cryptographic mechanisms that expose sensitive data.
- **Example**: Storing passwords in plaintext or using weak encryption algorithms like MD5.

3. Injection:

- **Description**: Inserting malicious code into a program, often through user inputs, to execute unintended commands or queries.
- **Example**: SQL injection, where an attacker can manipulate a database query by injecting SQL code.

4. Insecure Design:

- **Description**: Flaws resulting from the absence of security in the design of applications, often due to lack of security controls in the design phase.
- **Example**: No proper validation on inputs allowing for attacks like XSS.

5. Security Misconfiguration:

- **Description**: Improper configuration of security settings in applications, servers, or databases, exposing systems to attacks.
- **Example**: Leaving default accounts active, unnecessary features enabled, or error messages revealing too much information.

6. Vulnerable and Outdated Components:

- **Description**: Using libraries, frameworks, or other components with known vulnerabilities can introduce security risks.
- **Example**: Running an outdated version of a software library that is vulnerable to known attacks.

7. Identification and Authentication Failures:

- **Description**: Weak authentication mechanisms or improper session handling, which allow attackers to compromise user identities.
- **Example**: Allowing weak passwords or session hijacking due to insecure token handling.

8. Software and Data Integrity Failures:

- **Description**: Failures related to software updates, critical data, or CI/CD pipelines not being properly verified for integrity.
- **Example**: Allowing unsigned or untrusted software updates, which could lead to compromise.

9. Security Logging and Monitoring Failures:

- **Description**: Lack of sufficient logging, monitoring, or response mechanisms, leading to undetected attacks and delayed incident response.
- **Example**: Not logging failed login attempts or ignoring alerts for suspicious activity.

10. Server-Side Request Forgery (SSRF):

- **Description**: An attacker tricks a server into making unintended requests to other resources, potentially exposing sensitive internal systems.
- **Example**: Exploiting an API to make the server fetch unauthorized data from internal networks.

15. What is SSL Handshake?

    The network is important for office, home, and business networks. The problem is at the utmost places wireless communication is used or we can say the wireless network is used which is effortlessly hackable and the router can be freely exploited if not secured rightly. So there's a

need for security in the network. To fulfill this need we can use security protocols or cryptographic protocols to deliver authentication and data security.

16. What is a Cyber Kill Chain?
    The cyber kill chain is an adaptation of the military's kill chain, which is a step-by-step approach that identifies and stops enemy activity. Originally developed by Lockheed Martin in 2011, the cyber kill chain outlines the various stages of several common cyberattacks and, by extension, the points at which the information security team can prevent, detect or intercept attackers.

17. How does Traceroute work?
    A traceroute works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission are able to effectively transfer the data.

18. What is Incident response process?
    Incident Response Process: Establish a clear sequence of steps for incident detection, containment, eradication, recovery, and post-incident review. Ownership and Responsibility: Assign specific roles for each stage of the response process, with clear titles and contact details for each team member.

19. What is PKI?
    Public key infrastructure is an important aspect of internet security. It is the set of technology and processes that make up a framework of encryption to protect and authenticate digital communications.
    PKI uses cryptographic public keys that are connected to a digital certificate, which authenticates the device or user sending the digital communication. Digital certificates are issued by a trusted source, a certificate authority (CA), and act as a type of digital passport to ensure that the sender is who they say they are.
    Public key infrastructure protects and authenticates communications between servers and users, such as between your website (hosted on your web server) and your clients (the user trying to connect through their browser. It can also be used for secure communications within an organization to ensure that the messages are only visible to the sender and recipient, and they have not been tampered with in transit.
    The main components of public key infrastructure include the following:
    - **Certificate authority (CA):** The CA is a trusted entity that issues, stores, and signs the digital certificate. The CA signs the digital certificate with their own private key and then publishes the public key that can be accessed upon request.
    - **Registration authority (RA):** The RA verifies the identity of the user or device requesting the digital certificate. This can be a third party, or the CA can also act as the RA.
    - **Certificate database:** This database stores the digital certificate and its metadata, which includes how long the certificate is valid.
    - **Central directory:** This is the secure location where the cryptographic keys are indexed and stored.

- **Certificate management system:** This is the system for managing the delivery of certificates as well as access to them.
- **Certificate policy:** This policy outlines the procedures of the PKI. It can be used by outsiders to determine the PKI's trustworthiness.

20. What is SQL Injection?
    SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

21. What is Zero-day vulnerability?
    "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems. The unknown or unaddressed vulnerability is referred to as a zero-day vulnerability or zero-day threat.

22. What is the principle of least privilege?
    The principle of least privilege, also called "least privilege access," is the concept that a user should only have access to what they absolutely need in order to perform their responsibilities, and no more. The more a given user has access to, the greater the negative impact if their account is compromised or if they become an insider threat.

23. What is MITRE Attack Framework?
    The MITRE ATTACK Framework is a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework is meant to be more than a collection of data: it is intended to be used as a tool to strengthen an organization's security posture.

24. What is Zero Trust Framework?
    Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

25. What are some common threat vectors?
    Common threat vectors in cybersecurity refer to the pathways or methods that adversaries use to breach systems or networks. There are some types of threats vectors.
    1. **Phishing**: Fraudulent attempts to obtain sensitive information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in emails, messages, or websites.

2. **Malware**: Malicious software (e.g., viruses, ransomware, spyware, trojans) that compromises systems by exploiting vulnerabilities, often delivered through emails, downloads, or compromised websites.
3. **Social Engineering**: Manipulating individuals into divulging confidential information through non-technical means, such as impersonation or psychological manipulation.
4. **Insider Threats**: Employees or contractors with access to sensitive information intentionally or unintentionally compromising security, either by leaking data or exploiting their access for malicious purposes.
5. **Weak Passwords**: Poor password practices, like using weak or reused passwords, can allow attackers to easily guess or brute-force credentials and gain unauthorized access.
6. **Software Vulnerabilities**: Unpatched or outdated software with security flaws that can be exploited by attackers to gain unauthorized access, escalate privileges, or deploy malware.
7. **Unsecured Wi-Fi Networks**: Public or unprotected wireless networks can be exploited by attackers to intercept data or perform man-in-the-middle attacks.
8. **Distributed Denial of Service (DDoS)**: Attackers flood a network or website with excessive traffic, causing services to become unavailable to legitimate users.
9. **Third-party Vendors**: Insecure third-party software, hardware, or service providers with access to systems can introduce vulnerabilities that attackers can exploit.
10. **Mobile Devices**: The growing use of mobile devices can lead to exposure if these devices are not properly secured, with risks including malware, phishing, or lost/stolen devices.
11. **Cloud Security Gaps**: Misconfigurations or poor access control in cloud services can expose sensitive data to unauthorized users or malicious actors.

26. What is ARP?

    Address Resolution Protocol (ARP)is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

    When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.

    The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

    If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

27. What is DHCP?

    DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cell phones, etc. is an application layer protocol that is used to provide.

28. What are the HTTP response codes?
    HTTP response status codes **indicate whether a specific HTTP request has been successfully completed**. Responses are grouped in five classes: Informational responses (100 – 199) Successful responses (200 – 299) Redirection messages (300 – 399) Client error responses (400 – 499) Server error responses (500 – 599).

29. What is WAF (Web Application Firewall)?
    A **Web Application Firewall (WAF)** is a security solution that monitors, filters, and protects HTTP traffic to and from a web application. It acts as a shield between a web application and the Internet, helping to prevent various types of attacks, such as:
    1. **SQL Injection**: Attacks that exploit vulnerabilities in the application's database layer.
    2. **Cross-Site Scripting (XSS)**: Attacks that inject malicious scripts into web pages viewed by other users.
    3. **Cross-Site Request Forgery (CSRF)**: Attacks that trick users into submitting unwanted actions on a web application.
    4. **Distributed Denial of Service (DDoS)**: Attempts to overwhelm the application with traffic.

    Key Features of WAFs:
    - **Traffic Monitoring**: Analyzes incoming and outgoing web traffic for malicious activity.
    - **Threat Intelligence**: Utilizes known attack patterns and signatures to block attacks.
    - **Custom Rules**: Allows organizations to create specific rules tailored to their application's needs.
    - **Session Protection**: Protects user sessions from hijacking and other unauthorized actions.
    - **Logging and Reporting**: Provides insights and analytics on traffic patterns, potential threats, and incidents.

    Deployment Types:
    1. **Cloud-based WAF**: Deployed as a service in the cloud, offering scalability and ease of management.
    2. **On-Premises WAF**: Installed locally on the organization's servers, providing greater control over security policies.
    3. **Hybrid WAF**: Combines both cloud and on-premises deployment.

    Benefits of Using a WAF:
    - **Improved Security**: Protects against a variety of web application attacks.
    - **Compliance**: Helps organizations meet regulatory requirements related to data protection.
    - **Performance Enhancement**: Can optimize web traffic and improve application performance through caching and load balancing.

30. Questions on Ports number:-

HTTP	80
HTTPS	443
DNS	53(OR UDP)
SNMTP	25
REMOTE DESKTOP	3389
FTP	21
SMB	445

TOP 30 Cybersecurity Interview Questions [For Freshers]