CYBER SECURITY INTERVIEW QUESTIONS FOR (BEGINNERS)

1. What is cybersecurity, and why is it important?

Cybersecurity protects computer systems, networks, and data from theft, damage, or unauthorized access. It's important to safeguard sensitive information, maintain privacy, prevent financial losses, and protect critical infrastructure from cyber threats.

2. Define the terms Virus, Malware, and Ransomware.

- Virus: A program that replicates itself and spreads to other files or systems, often causing harm.
- Malware: A broader term encompassing any malicious software that disrupts or gains unauthorized access to computer systems.
- Ransomware: A malicious software encrypting files or computer systems and requesting a ransom for their decryption.

3. Explain the difference between a Threat, Vulnerability, and Risk in cybersecurity.

- Threat: Any potential danger or harmful event that can exploit vulnerabilities and negatively impact security.
- Vulnerability: Weaknesses or gaps in security measures that threats can exploit.
- Risk: The probability of a threat capitalizing on a vulnerability and the potential consequences or damage it may inflict.

4. What is Phishing? Provide an example.

- Phishing: A cyberattack in which malicious actors employ deceptive emails or messages to deceive individuals into disclosing sensitive information.

- Example: An email claiming to be from a bank, requesting the recipient to provide their login credentials by clicking a link that leads to a fake website.

5. How do firewalls protect network security?

- Firewalls serve as protective barriers, overseeing and screening both inbound and outbound network traffic in accordance with established security regulations.
- They block unauthorized access and help prevent malicious data from entering or leaving a network.

6. What is a VPN and why is it used?

- A Virtual Private Network encrypts and secures internet connections, ensuring privacy and anonymity.
- It protects data from eavesdropping, accesses restricted content, and enhances public Wi-Fi security.

7. Explain the concept of a secure Password.

- A secure password is complex, lengthy, and difficult to guess.
- It comprises a combination of uppercase and lowercase letters, numbers, and special characters, with the requirement that this combination should be distinct for every individual account.

8. What are the common techniques for securing a computer network?

Techniques include using strong passwords, regular updates and patch management, implementing firewalls, using intrusion detection systems, and conducting security audits.

9. What is two-factor authentication, and why is it important?

- Two-factor authentication enhances security by necessitating users to furnish two distinct forms of verification, typically a password and a temporary code, thereby bolstering protection.

- It's important because even if a password is compromised, unauthorized access is prevented without the second factor.

10. Define the terms Encryption and Decryption.

- **Encryption**: Converting plaintext data into a coded format to protect it from unauthorized access.
- **Decryption**: Converting encrypted data back into its original, readable form.

11. What is SSL encryption?

- SSL (Secure Sockets Layer) encryption is a protocol that ensures secure data transmission between a user's web browser and a website server, protecting data during transit.
-

12. What is the difference between IDS and IPS?

- IDS (Intrusion Detection System): Monitors network traffic and generates alerts when suspicious activity is detected.
- IPS (Intrusion Prevention System): Not only detects but also actively blocks or prevents suspicious network activity.
-

13. What is social engineering? Give an example.

- Social engineering manipulates individuals to disclose confidential information or perform actions for malicious purposes.
- Example: Pretending to be a trusted colleague and asking for login credentials over the phone.

14. What are cookies in a web browser?

Cookies are stored by websites on a user's device. They are used to track user preferences, session information, and provide a personalized browsing experience.

15. What is a DDoS attack and how does it work?

A Distributed Denial of Service (DDoS) attack inundates a target server or network with excessive traffic originating from numerous sources, making it inaccessible to genuine users.

16. Explain what a security policy is.

A security policy comprises a collection of formally documented regulations, recommendations, and protocols that delineate an organization's methods to safeguard its information, assets, and technological resources.

17. What is the difference between symmetric and asymmetric encryption?

- Symmetric Encryption uses a similar key for encryption and decryption.
- Asymmetric Encryption employs a pair of keys, one public and one private. Data that is encrypted with one key can only be deciphered using the complementary key.

18.How can you prevent a Man-In-The-Middle attack?

- Use secure communication protocols, verify digital certificates, and avoid public Wi-Fi for sensitive transactions. Implementing strong encryption also helps.

19. What is a honeypot in cybersecurity?

A honeypot is a decoy system or network designed to attract attackers. It allows security professionals to study their tactics, techniques, and motivations.

20. Explain the concept of a digital signature.

A digital signature employs cryptographic methods to confirm the genuineness and unaltered state of a digital document or message, assuring both the sender's authenticity and the content's integrity.

21. What is a brute force attack?

It involves attackers employing a trial-and-error approach to find a password or encryption key by systematically testing every conceivable combination until they discover the correct one.

22. What are the common cyber threats today?

Common threats include malware, ransomware, phishing, DDoS attacks, insider threats, and zero-day vulnerabilities.

23. What are the common cyber threats today?

Common threats include malware, ransomware, phishing, DDoS attacks, insider threats, and zero-day vulnerabilities.

24. Explain the concept of Public Key Infrastructure (PKI).

PKI is a system of cryptographic techniques that enables secure communication over an insecure network. A public key and a private key pair are employed for various cryptographic operations such as encryption, decryption, the creation of digital signatures, and the validation of public keys through the use of certificate authorities (CAs) to ensure their authenticity.

25. What are the key elements of a strong security policy?

A strong security policy includes elements like access control, encryption, regular updates, user training, incident response plans, and compliance with relevant regulations.

26. Explain cross-site scripting and SQL injection.

XSS involves injecting malicious scripts into web applications, which can compromise user data. SQL Injection exploits vulnerabilities in SQL queries to manipulate a database. Both are forms of web application vulnerabilities.

27. What is a zero-day vulnerability?

It refers to a security vulnerability present in software or hardware that is undisclosed to the vendor and lacks an existing solution. This loophole can be leveraged by malicious actors before a remedy is created.

28. Explain the principles of ethical hacking.

Ethical hacking involves testing systems and networks for vulnerabilities to strengthen security. Principles include obtaining proper authorization, maintaining confidentiality, and responsible disclosure of findings.

29. What are the different types of network security?

Network security includes perimeter security, firewall protection, intrusion detection systems, VPNs, and network segmentation to safeguard data and resources.

30. Discuss the concept of risk assessment in cybersecurity.

Risk assessment in cybersecurity involves identifying, assessing, and prioritizing potential threats and vulnerabilities to make informed decisions on security measures.

31. What is incident response, and how is it managed?

Incident response encompasses a methodical strategy for handling and diminishing security incidents, encompassing key phases such as preparation, detection, containment, eradication, recovery, and knowledge acquisition.

32. Explain the principle of least privilege.

The Least Privilege principle limits the access of users and processes to the bare minimum required for their specific tasks, thereby minimizing the potential for unauthorized actions.

33. What is network sniffing?

Network sniffing is the practice of intercepting and analyzing network traffic to gather information, potentially for malicious purposes. It can be used for monitoring or attacks.

34. How do penetration testing and vulnerability assessments differ?

Penetration testing replicates real-world attack scenarios to discover vulnerabilities, whereas vulnerability assessments concentrate on scanning systems to detect recognized weaknesses.

35. What is a Security Operations Center (SOC)?

SOC is a centralized team responsible for real-time monitoring, detecting, and responding to security incidents.

36. How does Secure Socket Layer (SSL) work?

SSL protocol ensures secure data transmission between web browsers and servers using encryption, authentication, and data integrity checks.

37. Explain OSI Model?

The OSI model, or Open Systems Interconnection model, is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. These layers facilitate communication between different systems and devices over a network. Here are the layers, from top to bottom:

1. Application Layer: Interfaces directly with user applications (e.g., HTTP, FTP).

2. Presentation Layer: Translates data formats, handles encryption and decryption.

3. Session Layer: Manages sessions and controls the dialogue between applications.

4. Transport Layer: Ensures reliable data transfer, handles error correction (e.g., TCP, UDP).

5. Network Layer: Manages routing and addressing of data packets (e.g., IP).

6. Data Link Layer: Facilitates node-to-node data transfer and error detection (e.g., Ethernet).

7. Physical Layer: Concerns the physical transmission of data over a medium (cables, signals).

38. What is ARP?

ARP, or Address Resolution Protocol, is a network protocol used to map an IP address to a physical MAC (Media Access Control) address on a local area network (LAN). When a device wants to communicate with another device on the same network, it uses ARP to discover the MAC address associated with the target IP address.

Key Functions of ARP:

1. Address Resolution: Converts an IP address to a MAC address.

2. ARP Request: A broadcast message sent by a device asking "Who has this IP address?"

3. ARP Reply: The device with the requested IP address responds with its MAC address.

39. what is TCP 3-way Handshake ?

The TCP 3-way handshake is a process used to establish a reliable connection between a client and a server. It involves three steps:

1. SYN: The client sends a SYN (synchronize) message to the server to initiate the connection.

2. SYN-ACK: The server responds with a SYN-ACK (synchronize-acknowledge), acknowledging the client's request and offering its own connection setup.

3. ACK: The client sends an ACK (acknowledge) to confirm the connection is established.

40. Explain? Types of Hackers?

Hackers can be categorized into several types based on their motives and methods. Here are the main types:

1. White Hat Hackers: Ethical hackers who use their skills to help organizations improve security. They often conduct penetration testing and vulnerability assessments.

2. Black Hat Hackers: Malicious hackers who exploit systems for personal gain, such as stealing data, spreading malware, or causing damage.

3. Gray Hat Hackers: Hackers who may violate laws or ethical standards but without malicious intent. They might expose vulnerabilities without permission, often informing the organization afterward.

4. Script Kiddies: Inexperienced hackers who use existing scripts or tools developed by others to launch attacks. They typically lack advanced skills and knowledge.

5. Hacktivists: Hackers who use their skills for political or social activism, often to promote a cause or protest against organizations.

6. State-Sponsored Hackers: Government-affiliated hackers engaged in espionage, cyber warfare, or surveillance against other nations or organizations.

7. Cybercriminals: Hackers who engage in illegal activities for profit, including identity theft, financial fraud, and ransomware attacks.

41. What is DHCP?

DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network settings (like gateway and DNS) to devices on a network. This eliminates the need for manual configuration and ensures devices can communicate easily on the network.

42. What is Cyber Kill Chain?

The Cyber Kill Chain is a framework developed by Lockheed Martin to describe the stages of a cyberattack, helping organizations understand and defend against threats by breaking down the attack process. It is a step-by-step model of how attackers move through a network to achieve their objectives, such as data theft or system compromise.

Stages of the Cyber Kill Chain:

1. **Reconnaissance**: Attackers gather information about the target, such as identifying vulnerabilities or researching employees.

2. **Weaponization**: The attacker creates malicious payloads, such as malware or exploit tools, to use in the attack.

3. **Delivery:** The attacker sends the malicious payload to the target via methods like phishing emails, malicious links, or infected files.

4. **Exploitation**: The attacker exploits a vulnerability in the target system to execute the malicious code or gain access.

5. **Installation:** Malware or backdoors are installed on the target system, allowing the attacker to maintain persistent access.

6**. Command and Control (C2):** The attacker establishes a communication channel to remotely control the compromised system.

7. **Actions on Objectives:** The attacker performs their end goal, such as data exfiltration, system disruption, or espionage.

Purpose of the Cyber Kill Chain:

Understanding the steps in the Cyber Kill Chain helps defenders recognize where they can detect, respond to, and stop an attack, ideally before it reaches the final stage. It provides insight into how attacks unfold and can improve defence strategies.

43. Explain? Common Types of Cyber Attack.

Cyber Attacks are malicious actions aimed at compromising the security of systems, networks, or data. Here are some of the common types of cyberattacks:

1. **Malware**

Malware refers to malicious software designed to damage, disrupt, or gain unauthorized access to a computer system.

Examples:

Viruses: Infect files and spread from system to system.

Worms: Self-replicating malware that spreads without user interaction.

Trojans: Disguised as legitimate software, but when installed, can steal data or provide backdoor access.

Ransomware: Encrypts files and demands payment to restore access.

Spyware: Secretly monitors and collects information about users.

2. **Phishing**

Phishing is a social engineering attack where attackers impersonate a trusted entity (via emails, messages, or websites) to trick victims into divulging sensitive information such as passwords or financial details.

3**. Denial of Service (DoS) & Distributed Denial of Service (DDoS**)

These attacks overwhelm a system, server, or network with excessive requests, making it unable to respond to legitimate traffic.

DoS: Involves a single attacker flooding the target with traffic.

DDoS: Uses multiple compromised systems (botnets) to launch the attack, making it harder to defend.

4**. Man-in-the-Middle (MitM) Attack**

In this attack, the attacker secretly intercepts and alters communication between two parties without their knowledge.

Example: An attacker eavesdropping on communication in a public Wi-Fi network to steal login credentials or sensitive information.

5. **SQL Injection**

SQL Injection involves injecting malicious SQL queries into input fields (such as login forms or search boxes) to manipulate a database.

Goal: Access, modify, or delete database records, often exposing sensitive data.

6. **Cross-Site Scripting (XSS)**

XSS attacks inject malicious scripts into trusted websites that then execute in the user's browser. These scripts can steal cookies, session tokens, or other sensitive data.

Example: Embedding malicious JavaScript in a comment section that runs when other users view the page.

7**. Password Attacks**

These attacks aim to obtain or crack a user's password.

Types:

Brute Force: Systematically guessing passwords using all possible combinations.

Dictionary Attack: Using common passwords or phrases to guess the correct one.

Credential Stuffing: Using stolen usernames and passwords from one breach to attempt logins on other sites.

8**. Zero-Day Exploit**

A zero-day exploit targets a software vulnerability that is unknown to the vendor or has not been patched yet. Attackers use this gap to compromise systems before the vendor can release a fix.

Example: Exploiting a vulnerability in a browser to inject malware.

9. **Advanced Persistent Threat (APT**)

APTs are prolonged and targeted attacks where adversaries infiltrate a network and remain undetected for a long time. The goal is often espionage or theft of sensitive information.

Example: Nation-state actors gaining long-term access to government or corporate networks for surveillance.

10. **Social Engineering**

This involves manipulating individuals into divulging confidential information by exploiting human psychology.

Types:

Pretexting: Creating a fake scenario to steal sensitive information.

Baiting: Offering something enticing (like free software) to trick users into compromising their systems.

Tailgating: Gaining unauthorized physical access to a building by following someone with legitimate access.

11**. Insider Threats**

Insider threats come from individuals within the organization who intentionally or unintentionally compromise security. These individuals often have authorized access to systems and data.

Example: A disgruntled employee leaking sensitive company data.

12**. Ransomware**

Ransomware is a type of malware that encrypts a victim's files, making them inaccessible, and demands a ransom for decryption.

Notable Example: The WannaCry ransomware attack that affected organizations globally.

13**. Drive-by Download Attack**

In a drive-by download, users accidentally download malware just by visiting a compromised website, without any active interaction like clicking a link or downloading a file.

Target: Outdated browsers or software with unpatched vulnerabilities.

14**. Session Hijacking**

Session hijacking involves stealing a user's session ID (usually from cookies) to impersonate the user and gain unauthorized access to a system.

Example: Taking control of a user's active session on a banking site to transfer money.

15. **DNS Spoofing (DNS Cache Poisoning**)

This attack alters DNS (Domain Name System) records to redirect users from legitimate websites to malicious sites. It can be used for phishing or delivering malware.

Example: Redirecting a bank's website to a fake page to steal login credentials.

16**. Credential Stuffing** Attackers use previously stolen usernames and passwords from other breaches to attempt to gain access to various services where users might reuse the same credentials.

44. What are the HTTPS Response Code?

HTTP response codes are status codes sent by a server to indicate the outcome of an HTTP request. They are grouped into five categories:

1. 1xx - Informational: The request is being processed.

100: Continue

101: Switching Protocols

2. 2xx - Success: The request was successfully received, understood, and accepted.

200: OK

201: Created

204: No Content

3. 3xx - Redirection: Further action is needed to complete the request.

301: Moved Permanently

302: Found (Temporary Redirect)

304: Not Modified

4. 4xx - Client Errors: The request contains bad syntax or cannot be fulfilled.

400: Bad Request

401: Unauthorized

403: Forbidden

404: Not Found

5. 5xx - Server Errors: The server failed to fulfill a valid request.

500: Internal Server Error

502: Bad Gateway

503: Service Unavailable

These codes help in diagnosing and handling the response from web servers.

45. What are NIDS and HIDS?

NIDS (Network Intrusion Detection System) and HIDS (Host Intrusion Detection System) are two types of intrusion detection systems used to monitor and analyze activities on networks and individual devices for suspicious behaviour or security breaches.

NIDS (Network Intrusion Detection System)

Purpose: Monitors network traffic for suspicious activities and potential intrusions.

HIDS (Host Intrusion Detection System)

Purpose: Monitors and analyses the behavior of individual hosts or endpoints for malicious activities.

46. What is Cryptography?

Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for.

47. What is the difference between Symmetric and Asymmetric encryption?

Basis of Comparison	Symmetric Encryption	Asymmetric Encryption
Encryption key	Same key for encryption & decryption	Different keys for encryption & decryption
Performance	Encryption is fast but more vulnerable	Encryption is slow due to high computation
Algorithms	DES, 3DES, AES and RC4	Diffie-Hellman, RSA
Purpose	Used for bulk data transmission	Often used for securely exchanging secret keys

48. What is the difference between VA(Vulnerability Assessment) and PT(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.

49. Explain CIA triad.

CIA stands for Confidentiality, Integrity, and Availability. CIA is a model that is designed to guide policies for Information Security. It is one of the most popular models used by organizations.

Confidentiality

The information should be accessible and readable only to authorized personnel. It should not be accessible by unauthorized personnel. The information should be strongly encrypted just in case someone uses hacking to access the data so that even if the data is accessed, it is not readable or understandable.

Integrity

Making sure the data has not been modified by an unauthorized entity. Integrity ensures that data is not corrupted or modified by unauthorized personnel. If an authorized individual/system is trying to modify the data and the modification wasn't successful, then the data should be reversed back and should not be corrupted.

Availability

The data should be available to the user whenever the user requires it. Maintaining of Hardware, upgrading regularly, Data Backups and Recovery, Network Bottlenecks should be taken care of.

50. What is a Firewall and why is it used?

A Firewall is a network security system set on the boundaries of the system/network that monitors and controls network traffic. Firewalls are mainly used to protect the system/network from viruses, worms, malware, etc. Firewalls can also be to prevent remote access and content filtering.

51. Explain SSL Encryption

SSL(Secure Sockets Layer) is the industry-standard security technology creating encrypted connections between Web Server and a Browser. This is used to maintain data privacy and to protect the information in online transactions. The steps for establishing an SSL connection is as follows:

1 . A browser tries to connect to the webserver secured with SSL

2 The browser sends a copy of its SSL certificate to the browser

3 The browser checks if the SSL certificate is trustworthy or not. If it is trustworthy, then the browser sends a message to the web server requesting to establish an encrypted connection

4 The web server sends an acknowledgment to start an SSL encrypted connection

5 SSL encrypted communication takes place between the browser and the web server

52. What steps will you take to secure a server?

Secure servers use the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorized interception. Here are four simple ways to secure server:

Step 1: Make sure you have a secure password for your root and administrator users

Step 2: The next thing you need to do is make new users on your system. These will be the users you use to manage the system

Step 3: Remove remote access from the default root/administrator accounts

Step 4: The next step is to configure your firewall rules for remote access

53. What is Port Scanning?

Port Scanning is the technique used to identify open ports and service available on a host. Hackers use port scanning to find information that can be helpful to exploit vulnerabilities. Administrators use Port Scanning to verify the security policies of the network. Some of the common Port Scanning Techniques are:

1 Ping Scan

2 TCP Half-open

3 TCP Connect

4 UDP

5 Stealth Scanning

54.What is a Botnet?

A Botnet is a number of devices connected to the internet where each device has one or more bots running on it. The bots on the devices and malicious scripts used to hack a victim. Botnets can be used to steal data, send spams and execute a DDOS attack.

55. Explain XSS attack and how to prevent it?

XSS (Cross-Site Scripting) is a cyberattack that enables hackers to inject malicious client-side scripts into web pages. XSS can be used to hijack sessions and steal cookies, modify DOM, remote code execution, crash the server etc. You can prevent XSS attacks by using the following practices:

Validate user inputs

Sanitize user inputs

Encode special characters

Use Anti-XSS services/tools

Use XSS HTML Filter