INFOSECTRAIN

TOP CYBER SECURITY

INTERVIEW QUESTIONS

CYBER SECURITY

Cybersecurity is the only area of IT that has not experienced a recession yet. Demand brings competition. It is essential for handling data breaches, effectively safeguarding sensitive data, and reducing risk. While possessing the required Cybersecurity abilities is the first step, passing the interview is an entirely different story. Cybersecurity interview questions and answers to assist you in acing interview successfully.

Interview Questions

1 What exactly is Cybersecurity?

Cybersecurity is concerned with preventing hackers from accessing electronic data on websites, networks, or devices. Cybersecurity experts assist in maintaining data security and accessibility through cutting-edge technology and complex procedures.

2 Which skills are necessary for a Cybersecurity professional?

Understanding network and endpoint threat mitigation are two essential skills for Cybersecurity professionals. A Cybersecurity professional must understand computer networks and cloud server security.

3 Define hacker?

An individual who violates a computer system is known as a hacker. Hacking can be done for various objectives, such as installing malware, stealing or destroying data, disrupting services, etc.

4 What is Cryptography?

Cryptography" comes from the Greek word kryptos, which means hidden. The study of secure communication methods, such as encryption, which restrict access to message contents to the sender and intended receiver, is known as cryptography.

5 What's the most common type of Cyberattack?

A phishing attack is the most common Cyberattack because it is simple to execute and surprisingly powerful.

6 What is a three-way handshake?

A three-way handshake (also known as TCP-3way handshake) is a mechanism to establish a connection between the client and server over a transmission control protocol/ internet protocol (TCP/IP) network. In this mechanism, the client and server send each other the synchronization and acknowledgment packets before an actual data transmission occurs.

7 Define a firewall?

A firewall is a program that filters both incoming and outgoing traffic networks according to a set of user-defined rules. A firewall's general goal is to lessen or completely stop undesirable network communications while enabling all lawful communication to proceed without interruption.

8 How do you configure a firewall?

A phishing attack is the most common Cyberattack because it is simple to execute and surprisingly powerful.

Username/password

Change a firewall device's default password.

Remote management

Disable the remote administration feature.

Configuration

Configure correct port forwarding for some applications, such as a web server or FTP server, to function effectively.

Server for DHCP

In the absence of disabling the firewall's DHCP, installing a firewall on a network with a DHCP server will cause a conflict.

Logging

Ensure logging is enabled and learn how to view logs to fix firewall problems or potential assaults.

Policies

Ensure the firewall is set up to enforce sound security regulations. You should also have strong security policies.

9 What function do antivirus sensor systems serve?

Antivirus software detects, stops and removes viruses from a computer. After installation, most antivirus programs run in the background to provide real-time protection against Cyberattacks.

10 What is security auditing?

Security auditing is considered one of the most effective ways to keep a system's integrity. Establishing the proper level of auditing for your environment should be a component of the overall security plan.

11 How do encryption and hashing differ?

The purpose of hashing and encryption are distinct. While hashing is a one-way procedure that converts data into the message digest, which is irreversible, encryption comprises both the encryption and decryption process.

12 Define a VPN?

A virtual private network, or VPN, is a service that aids in maintaining your online privacy. A VPN connects your computer to the Internet in a secure, encrypted manner, by creating a secure, encrypted tunnel for your data and conversations while you use public networks.

13 What are the possible response codes from a web application?

1xx – Informational responses

2xx – Success

- **3xx – Redirection**
- **4xx – Client-side error**
- **5xx – Server-side error**

14 What is data leakage?

Data leakage is the unauthorized transfer of information from an organization to an outside source via Hard Discs, USB storage devices, mobile phones, and other devices. This data may be physically or electronically leaked; it refers to the exposure or transmission of an organization's sensitive data to the external recipient.

15 What is SSL, and why is it important?

SSL is a data encryption protocol that enables secure communication between a web server and a web browser. Businesses and organizations must add SSL certificates to their websites to secure online transactions and protect client information.

16 Explain Two-factor Authentication with an example?

The second layer of security is added to your online accounts by two-factor authentication (2FA). For account

access, you need more than just your username and password; you also need access to something yours to obtain the additional log in credential.

Example-Using two different factors like a password and a one-time password (OTP) sent to a mobile phone via SMS is two-factor authentication.

17 What is a Cross-Site Scripting XSS attack?

Cross-site scripting (XSS) attack is something in which an attacker inserts harmful executable scripts into the source code of a reliable website or application. Attackers frequently start an XSS attack by giving users a malicious link and convincing them to click it.

18 How can identity theft be prevented?

- Use cryptic language.
- You might also give free online tools an attempt to generate passwords almost impossible to crack.
- Make sure all your passwords contain a combination of capital and lowercase letters, numbers, and other symbols like hyphens or punctuation marks.
- Never use the same password twice.

access, you need more than just your username and password; you also need access to something yours to obtain the additional log in credential.

Example-Using two different factors like a password and a one-time password (OTP) sent to a mobile phone via SMS is two-factor authentication.

19 How to Identify a DDoS Attack?

A website or program abruptly slowing down or failing to function is the most noticeable sign of a DDoS attack. However, other variables, such as increases in genuine traffic, problems with the hardware infrastructure, and a host of others, can also lead to the same issues.

20 Describe a botnet?

A computer network that has malware infections and is managed by a bot herder is referred to as a botnet. The individual who works the botnet infrastructure is known as the “bot herder.” A bot is any solitary device part of a botnet network.

21 What is ethical hacking?

Ethical hacking is a lawful effort to gain unauthorized access to a computer system, application, or data. To carry out ethical hacks, copies of malicious attackers' tactics and actions are used.

22 What is the difference between Symmetric and Asymmetric encryption?

Symmetric Key Encryption

Encryption changes a message's format so no one can read it. The message is encrypted using a key in symmetric-key encryption, and the same key is also used to decrypt the message, making it simple to use but less secure. A secure way must be used to pass the key from one party to another.

Asymmetric Key Encryption

Public and private essential encryption techniques are the foundation of asymmetric key encryption. The communication is encrypted and decrypted using two distinct keys. Although slower, it is more secure than symmetric key encryption.

23 What is a CIA triad?

The CIA (confidentiality, integrity, and availability) triangle is a methodology for handling information security rules inside an organization.

Confidentiality

A set of regulations restricting access to information is known as confidentiality.

Integrity

This guarantees the accuracy and dependability of the information.

Accessibility

It gives authorized users reliable access to data.

24 How does Traceroute work?

A Traceroute operates by transmitting Internet Control Message Protocol (ICMP) packets, which are received by every router involved in the data flow. The ICMP packets reveal if the routers utilized for the transmission can successfully transfer the data.

25 What is Port Scanning?

A port scan attack can be used by cybercriminals to identify open ports and determine whether they accept or reject data. It can also reveal whether a company employs firewalls or other active security measures.

The response that hackers get from a port when they send a message to it tells them whether the port is in use and whether it has any vulnerabilities that might be exploited.

Using the port scanning technique, businesses can also send packets to particular ports and examine the responses for potential vulnerabilities. To maintain the security of their network and systems, they can utilize tools like IP scanning, network mapper (Nmap), and Netcat.

Port scanning can provide information such as:

- Services that are running
- Users who own services
- Whether anonymous logins are allowed
- Which network services require authentication