eduonix

20 Most Asked Cyber Security Interview Questions

Questions for your Cybersecurity interview with answers that will land you the job!

Cybersecurity is the process of protecting crucial systems and sensitive information from digital attacks. Cybersecurity or IT security measures are designed to combat threats and unauthorised intrusions against networked systems and applications.
Cybersecurity, as a career, is on fast-track right now with a promising future ahead, partly because it is the need of the hour. But even if you have already learned the skills to make a career in cybersecurity, you still need to ace the interview and wow the recruiters with your answers.

Do you need to prepare for a cyber-security job interview?
Are you looking for tricks and tips to crack the interview? Don't worry, after reading this article, you'll know all the answers you need for acing your interview!

Here are some of the **most important interview questions** that you should know the answers to if you want a good job in the field of cybersecurity –

Q1. Explain Cybersecurity in simple terms and determine its objective.

Ans: Cybersecurity protects hardware, software, sensitive data and critical systems from threats and cyber attacks. The most essential and fundamental objective of cybersecurity is to protect data from any malicious threat or intent. For the application of this protection, the CIA principle is key - Confidentiality, Integrity and Availability.
If a security breach occurs, it translates that at least one and possibly all of these principles have been compromised.

Q2. What is the difference between threat, vulnerability and a risk?

Ans: Threat: A threat is any form of danger that has the potential to destroy or steal data, disrupt operations, or cause general harm. Malware, phishing, data breaches, and even unethical employees are examples of threats.
Vulnerability: A vulnerability is a defect in hardware, software, personnel, or processes that threat actors can use to achieve their objectives.

Risk: It is the probability that a threat agent successfully exploits a vulnerability, which can be calculated using the following formula: risk = probability of a threat * Impact of vulnerability. Risk management is the process of identification of all potential threats, analyzing their effects and determining the best course of action.
It's a never-ending process that periodically checks for new threats and vulnerabilities.

Q3. What does XSS stand for, and how can it be prevented?
Ans: It is a web security flaw that allows an attacker to manipulate how users interact with a susceptible application. Cross-site scripting flaws allow an attacker to impersonate a victim user and execute any actions that the user is capable of, as well as access any of the user's data. If the victim user has privileged access to the application, the attacker may be able to take complete control of the app`s functionality and data. Preventing cross-site scripting can be simple in some circumstances, but it can be much more difficult in others, depending on the application`s sophistication and how it handles user-controllable data. Encode user-controllable data in HTTP responses at the point where it is output to avoid it being perceived as active content. You can use the Content-Type and X-Content-Type-Options headers to ensure that browsers read HTTP responses in the way you intend, preventing XSS in HTTP responses that aren’t intended to contain any HTML or JavaScript.

Q4. What is a Firewall? What significance does it hold?
Ans: A Firewall is a network security program that is implemented on the boundaries of the systems & networks and monitors and controls the entire network traffic. It serves as a barrier between a LAN and the Internet. It is the first line of defence in protecting against threats. It is important for blocking unwanted content, helping prevent malicious files such as viruses, worms and malware and creating a secure network which protects every device within that network environment.

Q5. Differentiate between IDs and IPS.
Ans: The fundamental difference between them is that IDS i.e. Intrusion Detection System is a monitoring system, while IPS i.e. Intrusion Prevention System is a control system. IDS doesn't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address. IDS systems detect a variety of activities such as security policy violations, malware, and port scanners by comparing current network activity to a known threat database. If a packet represents a known security hazard, an IPS will proactively prohibit network traffic based on a security profile.

Q6. What are the different types of hackers?
Ans: Black hat hackers attempt to gain unauthorized access to a system to disrupt its operation or steal critical data. White hat hackers are also called ethical hackers. In the way of penetration testing and vulnerability analysis, they never intend to damage a system but try to discover loopholes in a computer or network system. The gray hat hackers combine elements of the black and white hat hackers. They act without corruption, but for pleasure they exploit a vulnerability in a computer system or network without the permission or knowledge of the owner. Their goal is to alert owners to the loopholes in hopes of receiving gratitude or a small reward.

Q7. State the differences between HTTPS, SSL, and TLS.
Ans: HTTPS stands for Hypertext Transfer Protocol Secure and its main job is to secure communications over a network. SSL is short for Secure Sockets Layer. TLS stands for transport layer security and is a successor protocol to SSL. Both SSL and TLS are encryption protocols on top of HTTP. You can elaborate the differences between the three and how network-related protocols are utilized to comprehend the inherent risks involved.

Q8. Differentiate between symmetric and asymmetric encryption.
Ans: In symmetric encryption, both encryption and decryption can be done using just one key, and the encryption is very fast. It is used when a huge amount of data needs to be transferred. The ciphertext is the same size or smaller than the plain text. Examples: AES, DES. In asymmetric encryption, it takes two keys to encrypt and decrypt data respectively, and the encryption is slow. It is used when a small volume of data needs to be transferred. The ciphertext is the same size or greater than the plain text. Examples: DSA, RSA. When compared to symmetric key encryption, asymmetric key encryption uses more resources.

Q9. What is VPN?
Ans: The term VPN refers to a virtual private network. It allows you to connect your computer to a private network by creating an encrypted connection that hides your IP address, so you can safely exchange data and access the Internet while protecting your identity online. A virtual private network or VPN is an encrypted connection between a device and a network across the Internet. The encrypted connection helps in the secure transmission of confidential data and protects against eavesdropping on traffic and allows users to work remotely. VPN technology is widely used in corporate environments. Examples: NordVPN, ZenMate.

Q10. What is the difference between VPN and VLAN?
Ans: Organizations use VLANs to consolidate devices that are distributed in multiple remote locations in a single broadcast domain. VPNs, on the other hand, are used to transfer secure data between two offices in the same organization or between offices in different companies. People also use it for their personal needs. A VLAN is a subtype of VPN. A VLAN is useful for segmenting a network into logical sections for ease of management, but it lacks the security features of a VPN. A virtual local area network minimizes the number of routers required and the cost of router deployment. A VPN improves the overall efficiency of a network.

Q11. What are the common types of cyber security attacks?
Ans: The common types of cyber security attacks are:-
Malware
- Cross-Site Scripting (XSS)
- Denial-of-Service (DoS)
- Domain Name System Attack
- Man-in-the-Middle Attacks
- SQL Injection Attack
- Phishing
- Session Hijacking
- Brute Force

Q12. What is the OSI model? Explain its different layers.
Ans: The OSI (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a network system. The OSI model characterizes computing functions in a universal set of rules and requirements to support interoperability between different products and software. In the OSI reference model, communication between a computer system is divided into seven different layers of abstraction: physical, data connection, network, transport, session, presentation, and application.

Q13. What do you mean by SQL Injection? How do you prevent it?
Ans: SQL injection is a typical attack in which fraudsters employ malicious SQL scripts to manipulate backend databases and get access to sensitive data. The hostile actor can see, edit, or remove important company data, customer lists, or customers' personal details contained in the SQL database after the attack is successful. The following practices can help you prevent SQL Injection attacks:
- Prepare statements ahead of time.
- Use Pre-defined Procedures
- Verify the user's input.

Q14. What do you mean by Shoulder Surfing?
Ans: Shoulder surfing is a form of physical assault that entails physically peering at people's screens while they type information in a semi-public space.

Q15. Differentiate between hashing and encryption.
Ans: Hashing is a method of converting data to a smaller fixed value known as the key, which is then used to represent the original data. Encryption is the technique of securely encoding data such that only the authorized user with the key or password can get the original data; for everyone else, it seems to be rubbish. The goal of hashing is to index and retrieve data from a database. The procedure is really quick. Encryption transforms data in order to keep it hidden from others. In comparison, hashing is more secure.

Q16. What do you mean by two-factor authentication?
Ans: Two-factor authentication (2FA), often also known as two-step verification or two-factor authentication, is a security method in which users validate their identity with two independent authentication factors. This procedure is done to better protect the user's credentials and the resources they have access to. Single-factor authentication (SFA), in which the user specifies only one factor, usually a password or passcode, offers a lower level of security than two-factor authentication (TFA). Since having the defendant's password alone is not sufficient to perform authentication verification, two-factor authentication adds an additional layer of security to the authentication process, making it difficult for attackers to gain access to devices or accounts in line with a person.

Q17. How can you avoid a brute force attack?
Ans: Brute Force attack can also be avoided by the following methods:-
Limit the number of failed login attempts.
- By altering the sshd_config file, you can make the root user unreachable via SSH.
- Instead of using the default port, change it in your sshd config file.
- Make use of Captcha.
- Limit logins to a certain IP address or range of IP addresses.
- Authentication using two factors
- URLs for logging in that are unique
- Keep an eye on the server logs.

Q18. What do you mean by Network Sniffing?

Ans: Sniffing is a technique for evaluating data packets delivered across a network. This can be accomplished through the use of specialized software or hardware. Sniffing can be used for a variety of purposes, including:

- Capture confidential information, such as a password.
- Listen in on chat messaging
- Over a network, keep an eye on a data package.

Q19. What do you mean by System Hardening?

Ans: In general, system hardening refers to a set of tools and procedures for managing vulnerabilities in an organization's systems, applications, firmware, and other components. The goal of system hardening is to lower security risks by lowering potential attacks and compressing the system's attack surface. The many types of system hardening are as follows:

- Hardening of the application
- Hardening the server
- Hardening the network
- Hardening of databases
- Hardening of the operating system

Q20. What do you mean by ARP poisoning?

Ans: Address Resolution Protocol Poisoning is a sort of cyber-attack that uses a network device to convert IP addresses to physical addresses. On the network, the host sends an ARP broadcast, and the receiver machine responds with its physical address. It is the practice of sending bogus addresses to a switch so that it can associate them with the IP address of a legitimate machine on the network and hijack traffic.

With these answers in your hands, you can pass any cybersecurity interview with minimal effort. So go get that job now and thank us later!

Learn Cyber Security With Global Experts and Kickstart Your Career in Cyber Security Field.

BUY 1 GET 1 FREE

Master the art of neutralizing all types of data breaches!
Get trained for White Hat Hacking, Pen Testing, Encryption, Network Security, Cloud Security, DevSecOps & other essential concepts with our **Advanced CyberSecutity E-degree Program.**

Real-World Projects you will work on.

- Extracting leaked credentials from network traffic
- DevSecOps Policy Creation
- Prevention Techniques inhouse & Enterprise
- Signature generation using Hash algorithms
- Review of Noteable Breaches in Cloud Security
- Website hacking using Metasploit

What You will Get

- 20+ Hours of Premium Video Content
- Online and self-paced
- 10+ Real-World Projects
- Certification
- Get Lifetime Access
- Mentorships
- Lifetime Free Updates and Support
- Job Assistance
- Exams and Quizzes

Learn Risk-Free with our “30 Days No Question Asked Money back guarantee”

BOGO OFFER Sitewide

LINK IN CAPTION

eduonix