**21 Most Asked Cyber Security Interview Questions**

According to an article published by Forbes, the need for Cyber Security personnel will constantly increase at a rate of 37% per year, at least until 2022.  This is why a career in Cyber Security is big these days. With more people trying to enter this field, writing about Cyber Security Interview Questions was inevitable, as we at Digital Vidya aim to make career growth easy for our readers.

Greater the influx and usage of internet, greater becomes the risk attached to it. The Internet has always been prone to risk and hacking, which makes working on it, or with it, a challenge for any business using it.

[*Check our our top rated Cyber Security Course!*](https://www.digitalvidya.com/cyber-security-course/)

Quality information on  Cyber Security Interview Questions on the internet is not abundant. That is primarily because, to qualify any cybersecurity interview, just searching for interview questions on cybersecurity won’t do. You need to demonstrate knowledge, experience, and skill that match the job requirements of this field.

On the other hand, there may be a very specific requirement from a job position. The company might want to make you work on the firewall or information security for example, so the interview for these roles will be very different quite naturally. But here we list the most asked cybersecurity interview questions that are always on the cards as you sit in the interview room.

**Most Asked Cyber Security Interview Questions by the HR**

As with any other job position, there would be an HR round of interview. This is done in order to ascertain the level of commitment that the candidate has. Securing basic background information and studying his/her personality to analyze a candidate’s fitness with regards to the culture of the organization is another purpose of this interview.

Cyber Security Questions asked by the HR

Some tricky questions that you need to be prepared for in the HR round of a cybersecurity interview are as follows:

**1. Why are you looking for a new role?**

**Ans:** Here you need to be honest as any deceitful answer will prove fatal in the long run. The answer to this question helps you to set your expectations clearly to the interviewer. You might be worn out at your previous job and might be looking look for a more relaxing role.

However, the position you are applying for might demand much more efforts than usual. If at this moment you try to answer the question by saying that you are looking for more responsibility, you definitely may land up with an offer, but you will regret joining the job later.

It is best to explain your motivation to join the job and your interest in the company you have applied for. Research both the role and the company and show that you are there to bring some positive energy into the organization.

**2. What are your greatest strengths and your greatest weaknesses?**

**Ans:** It is a typical question that every HR loves to ask. Take your time to explain your strengths by quoting examples from the previous work you had undertaken and in case you are a fresher, talk about the projects at your university.

Talk at length about the ways in which your leadership skills and proactiveness at work can be proven. You are free to talk about your relationship building and team skills here. Just remember to back every claim with a relevant example.

Most people tend to get a bit worried about answering the question about their weaknesses. The best way to answer this question is by talking about a couple of your weaknesses and then adding in the measures you are taking to improve on these loopholes.

**Most Asked Cyber Security Interview Questions for Freshers**

Cyber Security Interview Questions for Freshers

The greatest skill that would be analyzed in any cybersecurity interview is an aspirant’s knowledge of technology. This would be the real test of an inexperienced applicant in any given cybersecurity interview. Some of these cybersecurity interview questions for freshers might be very basic and theoretical, however, there would be others that will be geared towards technicalities and application. Here we list five most important interview questions on cybersecurity for freshers.

**1. What is the difference between HTTPS, SSL, and TLS?**

**Ans:** A hiring manager would want to understand the theoretical clarity of the aspirant. So, it is no brainer that you would need to depict clarity here.

HTTPS is hypertext transfer protocol which secures communications over a given network. SSL is quite different from it. SSL is a standard security technology which helps in creating an encrypted link between a server and a client. The clients, in this case, are mostly web browsers and web servers. A successor to SSL is the TLS. TLS is a name given to transport layer security.

Now, you would need to add that knowing about the differences in HTTPS, SSL and TSL would help a cybersecurity analyst to understand the inherent risks involved in each phase of data transmission.

**2. Is there a difference between a threat, vulnerability, and a risk?**

**Ans:** It is a vital question to answer as this demonstrates an aspirant’s readiness to work in the field of cybersecurity. Make the answer as simple as you can, there is a serious chance of getting caught up in a series of follow up questions.

Tell the interviewer that a threat comes from someone who is targetting you. Vulnerability comes from within your own organization. It is a name given to your weakness that may be caught by an external agent. A risk comes into the picture when you can’t properly mitigate your vulnerability.

**3. When there is a need to compress and encrypt data, which one should you do first and why?**

Compress and Encrypt Data

**Ans:** Since starting off with encrypting will make it hard for compression to show any visible effects, compression should precede encryption. If you have more knowledge about this affair, you can invoke that information to your benefit by systematically presenting it to the hiring manager.

**4. What is the best way to strengthen user authentication?**

**Ans:** Now here, you need to know that there no best and worst way to user authentication. Different platforms will require different levels of authentication. You can ask a counter question by asking about the specific industry and the type of transaction that is to take place.

Based on this, you may recommend a two-factor authentication or even a non-repudiation styled authentication. But remember, you should always be prepared to answer the ways of implementation as well.

**5. Explain a traceroute?**

**Ans:** A traceroute, which is sometimes also called a tracert, is used to know instances where the breakdown of communications occurs. It helps to determine the routers you come across as you move towards your final destination. This easily helps in tracking abnormalities.

For a fresher, as stated earlier, theory plays an important role for a good performance at presenting himself well for interview questions on cybersecurity.So, revise your concepts well before going to an interview.

**6. What is the difference between Asymmetric and Symmetric encryption?**

**Ans:**

|  |  |  |
| --- | --- | --- |
| **Point of Distinction** | **Symmetric Encryption** | **Asymmetric Encryption** |
| Encryption key | Symmetrical Encryption is a simple kind of encryption that involves only one secret key for encryption and decryption | Asymmetric encryption uses two keys for encryption and decryption. |
| Performance | Execution is fast in Symmetric encryption. | Due to high computation, execution is slow in Asymmetric Encryption. |
| Algorithms | DES, 3DES, AES, and RC4 | Diffie-Hellman, RSA |
| Usage | Symmetric encryption is used for the transmission of bulk data. | Asymmetric encryption is used for exchanging secret keys safely. |

**7. What is the CIA Triad?**

**Ans:** CIA stands for confidentiality, integrity and availability and is also known as CIA triad. It is a specially designed model for guiding policies & evaluating information security within an organization.

**(i) Confidentiality** – To keep information secret.  
**(ii) Integrity** – To assure that the information is trustworthy & accurate.  
**(iii) Availability** – To ensure that the information is available to authorised parties.

**8. What is the difference between IPS and IDS System?**

**Ans:**

|  |  |  |
| --- | --- | --- |
| **Point of Distinction** | **IDS** | **IPS** |
| Full Form | Intrusion Detection System | Intrusion Prevention System |
| Detection and Action | IDS just detects the intrusion & leaves the rest to the administrator to take further action. | IPS detects the intrusion & takes further action to prevent the intrusion. |
| Purpose | IDS monitors, audits and reports network malicious activities. | IPS provides protection to assets, resources, data, and networks. |

**9. What is XSS attacks and how will you prevent them?**

**Ans:** XSS or Cross-site scripting is a type of injection security attack or common attack vector in which an attacker injects malicious data into vulnerable & trusted websites. XSS does not target the application directly, rather it quite dangerous for web application users.

There are three ways to prevent XSS attacks:

**(i) Escaping:** This means taking the data an application has received to ensure that it’s secure.

**(ii) Validating Input:** This is the process of ensuring that the application is interpreting correct data & is preventing all types of malicious data from entering the site.

**(iii) Sanitizing:** This is the process of sanitizing user input. It scrubs the data & changes unacceptable user input to an acceptable format.

**10. What is CSRF?**

**Ans:** CSRF is Cross-Site Request Forgery. It is a method of attacking a website in which the attacker tricks the web browser by disguising as a legitimate & trusted user and executes an unwanted action on the website. This attack is generally executed by stealing the identity of an authorized existing user and then hacking the website.

**Most Asked Cyber Security Interview Questions for the Experienced**

For the experienced, the interview questions are going to get more technical and would be geared more towards application rather than mere theory. A candidate must show expertise in problem-solving, collaboration and project management.

Cyber Security Interview Questions for the Experienced

Here we list the top 5 most asked cybersecurity questions for the experienced cyber security professionals.

**1. What is a black box test? How is it different from a white box test?**

**Ans:** It is a common practice in some organizations that testing is done without giving any sort of information or details to the team working on a project. Such a way to test security is called Black Box Testing.

On the other hand, when information is given and all the details related to a security case shared, its termed as white box testing. Although, not very difficult to answer, nevertheless it is from the common interview questions on cybersecurity.

**2. Are there any levels of Data Classification? If yes, why are they important?**

**Ans:** Yes, there are various levels of Data Classifications and all of them need specific kinds of handling. Based on severity and vitality of the data stored, each type of classified data will require specific handling procedures.

Some pieces of data are critical while others are not. The way in which data is classified will be different for different organizations, however, it generally comes under the following three categories:

1. **Top Secret** – Data which if leaked can rupture the organization’s functionality
2. **Confidential** – Data which is internal to the company
3. **Public** – Data that is not hidden rather is publically available

**3. Explain salting and its uses?**

**Ans:** Salting, if defined simply, is a process that extends the length of passwords by adding some special characters to the original password. However, one needs to understand the entire mechanism of salting to put it to use.

Salting is an excellent way to turn passwords stronger in a manner which makes cracking passwords very hard even if the actual passwords are weak.

**4. Why is DNS monitoring important?**

**Ans:** In the absence of DNS it would be extremely hard to find a website as you would need to memorise a full IP address. It also makes information regarding different domains easily recognizable. It is the perfect way to have a directory sort of a list on the internet.

**5. How do you take care of the Antivirus alerts?**

**Ans:** This is precisely one of the most frequently asked cybersecurity interview questions. To answer this particular question it is recommended to use your personal expertise. However, the first thing to do here is to check the AntiVirus policy and then the alert. If the alert is sourced from a legitimate file, then be directly whitelisted. But if the alert is from a malicious source, then it should be deleted. Moreover, the AntiVirus should be finetuned and updates so as to reduce alerts.

**6. What is Data Leakage and what are the ways to prevent it?**

**Ans:** Data Leakage is an unauthorized process of transmission of data from the organization. The leakage of data can take place through various means like emails, unauthorised upload of data to public portals, removable drives etc. Data leakage can be prevented by closely monitoring traffic on all networks, mapping and tracking all the actions. Encrypting all the private, confidential and sensitive information is the next step to prevent data leakage.

**7. What is the easiest way to defend yourself from CSRF attacks?**

Defend yourself from CSRF attacks

**Ans:** An article on cybersecurity analyst interview questions and answers is incomplete without having this question. It is a very frequent question that is asked repeatedly in interview rooms. One advice that should be used across all technical questions is to keep your answer succinct and to the point in order to prevent from a volley of follow up questions.

Now coming back to the answer to the question, generally speaking, there are two ways to defend yourself from a CSRF attack. One where you allocate a random token with every request. The string of tokens generated makes a strong protective case. Else you can try using a new name for each field in a form. This will make you anonymous and thus there would be no path for CSRF attacks.

**8. What is DDoS Mitigation?**

**Ans:** DDoS Mitigation is the term that refers to the process of successfully protecting a targeted server or network from a distributed denial of service (DDoS) attack. A target victim is able to mitigate the threat by using specially designed network equipment.

DDoS Mitigation process is divided into 4 stages:

**(i) Detection** – In this stage, abnormal traffic flows are identified.  
**(ii) Diversion** – In this stage, abnormal traffic is misrouted from the target.  
**(iii) Filtering** – In this stage, the DDoS traffic is weeded out while clean traffic is passed on.  
**(iv) Analysis** – In this stage, security logs are reviewed to gather information about the attack.

**9. What is Black Hat, White Hat & Grey Hat Hacker?**

**Ans:** **Black Hat Hackers** are the ones who have extensive knowledge about hacking computer networks. They hack systems and software without any authority.  
**White Hat Hackers** are authorised hackers who hack systems to find and fix unethical actions. They are generally hired by the companies as security specialists.  
**Grey Hat Hackers** are the combination of Black & White Hat Hackers. They perform unauthorised activities to look for system vulnerabilities.

**Closing Remarks**

This post on cyber security engineer interview questions is not a list that is comprehensive, rather it based on the frequency of cybersecurity interview questions and answers. If you are a fresher, be prepared with lots of theory and if you are an experienced candidate, you need to provide examples and instances for everything you claim.

If you want to build a career in Cybersecurity, enroll yourself in this [Cybersecurity Course](https://www.digitalvidya.com/cyber-security-course/) and become a cybersecurity expert.