By OnlineInterviewQuestions.com

Information Assurance Interview Questions

Information assurance can be defined as measures applied so as to protect data/information and system holding that information by ensuring the five pillars of information assurance (namely CIA, Authentication and Non-Repudiation).

Information assurance can also be defined as a protection measure grown above the practice of information security and applies to data, either in electronic or physical forms together with their storage facilities.

If you pass the initial technical interview for posts relating to information assurance, the interview will go more technical and this post attempts to enlist a few tough information assurance interview questions.

Below is the list of 10 **Toughest Information Assurance Interview Questions** that will surely help you for the information security job that you are looking forward to join.

Q1. How are information protection and assurance different ?

Information assurance deals with protecting data and information system to keep the data reliable using non-repudiation techniques, backup and so on.

However, information protection simply deals with methods to keep the data safe through the use of encryption, security-related tools, and other ways.

Q2. What do you mean by CIA?

CIA is a basic principle of information assurance where C means Confidentiality- keeping data secure, I means Integrity – Keeping data intact and A means availability- keeping data accessible when required.

Q3. What do you mean by red team and blue team?

Succinctly put, the red team is the offensive and blue team is a defensive one. Red team needs to succeed only once to be able to achieve its target whereas Blue team needs to stay alert all the time to see if any breach has been made.

Q4. You have figured out a network problem, which needs to be solved immediately. But you find out that it is out of your jurisdiction. What will your next step be?

Security is a sensitive business. It is always advised to ask for privilege from higher authority. So, I would mail the admin with my Manager cc'd and keep the records if I am advised to solve the problem by one of those people.

Q5. What are Pros of bringing external security contractor to audit your system?

External auditors will be able to bring those missed and dangerous issues to notice. They will have a fresh look at your system and are more likely to discover issues that are unseen or doesn't want to be seen by insiders.

Q6. Which would be worse, false positive or False negative in case of detection ?

False positive means a detection of a packet that actually isn't malicious. But false negative is something that passes from Firewall and becomes an incident. False positive can be rectified by changing rule-set and manual testing. But false negative could cause compromise of an entire system. Thus, false negative is far dangerous than false positive detection by a firewall or an anti-virus software.

Q7. What do you mean by white box , grey box and black box testing?

In white box testing, a tester is provided with source code, network diagrams, programs running on the server side, or in a word 'complete privilege'. On the other hand, a black box tester will be given nothing -- he will have to perform or simulate an attack from a random outsider.

Q8. What do you mean by residual risk?

Literally, it means risk that remains. In infosec domain, it means acceptable risk for the company. Even if an issue is valid but due to usability problem and such, it's not surely going to be fixed.

Q9. When you press delete button, is a file actually deleted?

No, A file isn't deleted when you press that delete button. Actually what happens is your OS flips a bit telling that you don't need this file for now and can be overwritten, if required. You could use several tools to recover deleted files because they are not actually deleted but are ready to be overwritten.

Q10. What is ex-filtration?

It is a technique of social engineering, a way of extracting data from a company without getting noticed.