Top 12 Information Security Analyst Interview Questions & Answers

1) Explain what is the role of information security analyst?

From small to large companies role of information security analyst includes

- Implementing security measures to protect computer systems, data and networks
- Keep himself up-to-date with on the latest intelligence which includes hackers techniques as well
- Preventing data loss and service interruptions
- Testing of data processing system and performing risk assessments
- Installing various security software like firewalls, data encryption and other security measures
- Recommending security enhancements and purchases
- Planning, testing and implementing network disaster plans
- Staff training on information and network security procedures

2) Mention what is data leakage? What are the factors that can cause data leakage?

The separation or departing of IP from its intended place of storage is known as data leakage. The factors that are responsible for data leakage can be

- Copy of the IP to a less secure system or their personal computer
- Human error
- Technology mishaps
- System misconfiguration
- A system breach from a hacker
- A home-grown application developed to interface to the public
- Inadequate security control for shared documents or drives
- Corrupt hard-drive
- Back up are stored in an insecure place

3) List out the steps to successful data loss prevention controls?

- Create an information risk profile
- Create an impact severity and response chart
- Based on severity and channel determine incident response
- Create an incident workflow diagram
- Assign roles and responsibilities to the technical administrator, incident analyst, auditor and forensic investigator
- Develop the technical framework
- Expand the coverage of DLP controls
- Append the DLP controls into the rest of the organization
- Monitor the results of risk reduction

4) Explain what is the 80/20 rule of networking?

80/20 is a thumb rule used for describing IP networks, in which 80% of all traffic should remain local while 20% is routed towards a remote network.

5) Mention what are personal traits you should consider protecting data?

- Install anti-virus on your system
- Ensure that your operating system receives an automatic update
- By downloading latest security updates and cover vulnerabilities
- Share the password only to the staff to do their job
- Encrypt any personal data held electronically that would cause damage if it were stolen or lost
- On a regular interval take back-ups of the information on your computer and store them in a separate place
- Before disposing off old computers, remove or save all personal information to a secure drive
- Install anti-spyware tool

6) Mention what is WEP cracking? What are the types of WEP cracking?

WEP cracking is the method of exploiting security vulnerabilities in wireless networks and gaining unauthorized access. There are basically two types of cracks

- **Active cracking:** Until the WEP security has been cracked this type of cracking has no effect on the network traffic.
- **Passive cracking:** It is easy to detect compared to passive cracking. This type of attack has increased load effect on the network traffic.

7) List out various WEP cracking tools?

Various tools used for WEP cracking are

- Aircrack
- WEPCrack
- Kismet
- WebDecrypt

8) Explain what is phishing? How it can be prevented?

Phishing is a technique that deceit people to obtain data from users. The social engineer tries to impersonate genuine website webpage like yahoo or face-book and will ask the user to enter their password and account ID.

It can be prevented by

- Having a guard against spam
- Communicating personal information through secure websites only
- Download files or attachments in emails from unknown senders
- Never e-mail financial information
- Beware of links in e-mails that ask for personal information
- Ignore entering personal information in a pop-up screen

9) Mention what are web server vulnerabilities?

The common weakness or vulnerabilities that the web server can take an advantage of are

- Default settings
- Misconfiguration
- Bugs in operating system and web servers

10) List out the techniques used to prevent web server attacks?

- Patch Management
- Secure installation and configuration of the O.S
- Safe installation and configuration of the web server software
- Scanning system vulnerability
- Anti-virus and firewalls
- Remote administration disabling
- Removing of unused and default account

- Changing of default ports and settings to customs port and settings

11) For security analyst what are the useful certification?

Useful certification for security analyst are

- **Security Essentials (GSEC):** It declares that candidate is expert in handling basic security issues- it is the basic certification in security
- **Certified Security Leadership:** It declares the certification of management abilities and the skills that is required to lead the security team
- **Certified Forensic Analyst:** It certifies the ability of an individual to conduct formal incident investigation and manage advanced incident handling scenarios including external and internal data breach intrusions
- **Certified Firewall Analyst:** It declares that the individual has proficiency in skills and abilities to design, monitor and configure routers, firewalls and perimeter defense systems

12) How can an institute or a company can safeguard himself from SQL injection?

An organization can rely on following methods to guard themselves against SQL injection

- **Sanitize user input:** User input should be never trusted it must be sanitized before it is used
- **Stored procedures:** These can encapsulate the SQL statements and treat all input as parameters
- **Regular expressions:** Detecting and dumping harmful code before executing SQL statements
- **Database connection user access rights:** Only necessary and limited access right should be given to accounts used to connect to the database
- **Error messages:** Error message should not be specific telling where exactly the error occurred it should be more generalized.