Security Analyst Interview Questions (2018)

Q: What are the differences between Cyber Security and Info Security

Cyber Security Vs Info Security	
Cyber Security	**Information Security**
It is protection for cyberspace of threats & vulnerabilities.	InfoSec is defined as protection for information assets.
cybersecurity is a subset of information security	InfoSec is the preservation of confidentiality, available information & integrity.
It deals with cyber wars, frauds, crimes that with law enforcement	It does not deal with cyber crimes unless there is a loss of information against policy.
cybersecurity - professionals are 2 folded malware researchers & incident investigators	InfoSec - professional deals with security fundamentals.
It is protecting the hardware & data system from unauthorized access.	InfoSec is protecting the end user from different sorts of access.
It works in both online & offline modes.	The main purpose is online data security.
This job requires a degree of Cybersecurity, IT, CS or Engineering.	This job requires cryptography, InfoSec, Data Analysis & vast knowledge of Digital Information

Q: What is cyber security?
Cyber securities are defined as a group of processes, technologies and practices which are designed in a special way to protect computers, networks, access which are unauthorized and many more.

Q: What do you mean by Cross Site Scripting?
Cross Site Scripting generally tends to refer to an injected attack which is from the side of the client code, where, the one who is attacking has all the authorities in executive scripts which are malicious into an application of web or a website which is legitimate. Such kinds of attack are generally seen where the web application is making use of the non-encoded or non-validated inputs of the users inside the range of the output which is generated.

Q: What does Cyber security work for in a specific organization?
There are mainly three major reasons for which cyber security works:
1. Confidentiality: Whenever information is transmitted from one place to another, a certain level of secrecy is maintained, which is known as confidentiality.
2. Integrity: This means that whenever there is a need for change in any document stored beforehand or new, it can only be done by an authorized person with proper and secure mechanism.
3. Availability: Everything that is important should be readily available to the authorized people otherwise there will be no use of such information that is not available.

Q: What can you defend yourself from Cross Site Scripting attack?

Like any other injection attack, Cross Site Scripting attack can also be prevented by the use of the proper available sanitizers. Web developers have to have an eye on the gateways through which they receive information and these are the gateways which must be made as a barrier for malicious files. There are software or applications available for doing this, like the XSS Me for Firefox and domsnitch for Google Chrome. Also, the default web application firewall formula, popularly known as ModSecurity Plus will also do the job quite satisfactorily.

Q: What do you mean by a Botnet?

A botnet is basically known to be a network or a group of computers which are affected by malware and are being constantly monitored by a server which throws the commands. The one is in control of the botnet can impact some serious damage through all those linked computers affected with malware.

Q: Strike the difference between vulnerability, a risk and a threat?

These three terms are interlinked but they are very different from each other:

1. Vulnerability: If your security program has a breach or weakness then different threats can further exploit the program and thus hack into your system to access data that is stored securely.

2. Risk: If your system is not secure enough and has the chances of getting damaged or destruction along with loss of data when a threat exploits the vulnerability, it's under huge risk.

3. Threat: Something that is necessary for exploiting the vulnerability either knowingly or by accident in order to damage or destroy personal and official data.

Q: How can the two factor authentication be implemented for the public facing websites?

The two factor authentication or shortly abbreviated as 2FA acts as another or an extra seal on your already protected account with a password. This two factor authentication can be implemented on public-facing websites like Microsoft, Twitter, Apple, Google and LinkedIn. For enabling such services, one can easily go to settings and then to manage security settings. Here, you will find the option of enabling two factor authentications.

Q: Being a professional, what is more important Threats or Vulnerabilities?

Despite the advancements in the security systems with the years, the threats and vulnerabilities have only increased with each passing day. Assessing threats is still not under the control of any high-tech security team. Although, a threat rises from vulnerability, so if we have proper control over them, we can still try and control threats. Secondly, the type of threats remains same but the vulnerabilities are what keep on changing. Thus we need to focus on building something that has a proper defense mechanism and also can track down new vulnerabilities.

Q: What is the main point of consideration when it comes to the differences between the Stored XXS and the Reflected XXS?

In case of Stored XXS, since Stored XXS is stored in a page which is static, thus, it is directly pulled out and displayed to the user directly as per needed. On the other hand, in Reflected XXS, the user has to send a request first. Now, this request will start running on the browser of the victim's computer and then will reflect the results back from the website or the browser to the user who has sent the request.

Q: How does the HTTP control the State?
This is a tricky question. HTTP doesn't and will never control the state. Answers like cookies are still better. The job of the cookies is to provide a gateway to what HTTP can't do. In simpler terms, cookies serve as a hack to what HTTP fails to do.

Q: Describe the 3 major first steps for securing your Linux server.
Every system has its own security software's so for securing your Linux, the first three steps are:
1. Auditing: A system scan is performed using a tool called Lynis for auditing. Every category is scanned separately and the hardening index is provided to the auditor for further steps.
2. Hardening: After the audit is complete, the system is hardened depending on the level of security it further needs. It is an important process based on the decision of auditor.
3. Compliance: The system needs to be checked almost every day for better results and also lesser threats from security point of view.

Q: What are the techniques used in preventing a brute force login attack?
To avoid brute force login attacks, you generally have three kinds of techniques to go about. The first technique is to implement a policy for account lockout. In this method, an account will be locked out unless and until the administrator himself opens it. The second being progressive delays. In this method, after a few attempts of login, your account will stay locked for the next few number of days. Lastly, use a challenge-response test. This prevents any kind of automatic submissions on the login page.

Q: How can you defend yourself against CSRF attacks?
To defend yourself against CSRF attacks, you can opt for two available methods. Firstly, with every request try to include a random token. In this way a unique string of tokens will be generated which is a good safeguard. Secondly, for each field of form, try using different names. This will somewhat help you in becoming anonymous due to the entry of so many different names and thus will behave as a safeguard from CSRF attacks.

Q: What is the need for DNS monitoring?
The Domain Name System allots your website under a certain domain that is easily recognizable and also keeps the information about other domain names. It works like a directory for everything on the internet. Thus, DNS monitoring is very important since you can easily visit a website without actually having to memorize their IP address.

Q: Define the process of Salting and state the use of Salting.
Salting is that process where you extend the length of your passwords by using some special characters. In order to use salting, you must know the entire mechanism of salting and also, it is not that very difficult to be cracked by a person who already knows the concept of salting.
The use of salting is to make your passwords stronger and not easy to be cracked if you are someone who is prone to use of simple or ordinary words as passwords.

Q: State the difference between Symmetric Key Cryptography and Public Key Cryptography.
Both of these cryptography, that is, the Symmetric Key Cryptography and the Public Key Cryptography, does the same job of encrypting and decrypting, thereby, here lies the main

difference between them. Thus, the main difference between them is that in Symmetric Key Cryptography, only one key is put into use for encryption and decryption. On the other hand, in the case of Public Key Cryptography, they make use of two different keys. The public key for encryption and the private key for decryption. Generally, the Symmetric Key Cryptography is known to be faster and simpler.

Q: Describe the working of Traceroute.
Small Time To Live (TTL) values are transmitted through packets via traceroute. This process prevents the packets from getting into loops. After the router subtracts from the given packet's TTL, the packet immediately expires after the TTL reaches absolute zero. After that the sender is sent messages from Traceroute that exceed the time. When small values of TTL are used, the expiration happens quickly and thus the traceroute generates ICMP messages for identifying the router.

Q: How will you prevent the "Man-in-the-Middle" attack?
Commonly known as the "Bucket Brigade Attack", this attack happens through a man who is in between two different parties and controls the complete conversation without the two ends even realising that. The first method to prevent this attack would be to have an end to end encryption between both the parties. This way, they both will have an idea with whom they are talking because of the digital verification. Secondly, to prevent this, it is best to avoid open Wi-Fi networks and if it is necessary then use plugins like HTTPS, Forced TLS etc.

Q: How encoding, hashing and encryption differs from one another.
1. Encoding: Encoding converts the data in a desired format required for exchange between different systems. This doesn't convert it into a secret data, but usable data. It can be further decoded through the same tools when necessary.
2. Hashing: This serves for maintaining the integrity of a message or data. This way if any day it is hampered or changed, you will get to know.
3. Encryption: Encryption ensures that the data is secure and one needs a digital verification code or image in order to open or access it.

Q: SSL and HTTPS: Which is more secure?
SSL (Secure Sockets Layer) is a protocol which enables safe conversations between two or more parties over the internet. HTTPS (Hypertext Transfer Protocol Secure) is HTTP combined with SSL which provides you with a safer browsing experience with encryption. So, this is a very tricky question but SSL wins in terms of security.

Q: In encryption and compression of data during transmission, which of them would you do first? Justify with proper reasons.
If I had the option to encrypt and compress data, I would first compress the data. This is because of encrypting a data we obtain a stream of bits which are random. Now, these random bits become impossible to be compressed, in other words, they are incompressible. The reason to why these random bits become incompressible is because of the lack of any patterned structure. Compressing data always requires any specific pattern to be compressed which is lacked in random bits.

Q: Which is more secure? An open source project or a proprietary project?
The securities of these projects depends mainly on the size of the project, the total number of the developers who are working under this project and the one factor, which is most essential as well as important, is the control of the quality. Just the type of project won't determine its quality, the inside matter of the corresponding projects will matter.

Q: How do you acquire the Cybersecurity related news?
There are several places from where one might get the best cybersecurity news from but it is important to remember not all of it is correct and precise. So, for the best news related to cybersecurity you can go for Reddit, Team Cymru, Twitter etc. You have to be on top of the news count so that you don't wait for one to inform you about the recent changes.

Q: State the difference between Diffie-Hellman and RSA.
The basic difference which lies in both of these is the type of protocol they are. RSA is a protocol which is used for signing or encryption. On the other hand, Diffie-Hellman is a protocol which is used for exchange of key. Also, the RSA will expect that you have all the key materials with you beforehand, which is not the case with Diffie-Hellman.

Q: How to access Active directory from Linux?
It is quite surprising but you can use Active directory from Linux or iOS system or any other system apart from windows. The directory makes use of the SMB protocol which further can be accessed from a non-windows platform with the help of the Samba program.

Q: Why is using SSH from Windows better?
SSH is a connection used on different platforms on appliances for the best security. This hardens your security system against any threat and works well with Routers, SFTP and switches. It works the best with Windows although is compatible with other platforms too.

Q: How can you make the user authentication process more secure?
User authentication may sound very secure but it is not so secure. You need just the username and password to break into or hack into the authentication of that person. The main way of hardening is by choosing the password accordingly. You can either generate memorable passwords which are secure, passwords based on algorithm, making the use of password vaults, using authentications which are multifactor and highly secure and alternate embedding of the alphabets of a specific memorable word, are the best ways of hardening user authentication.

Q: Is SSL enough for your security?
SSL is meant to verify the sender's identity but it doesn't search in a hard way for more hazards. SSL will be able to track down the real person you are talking to but that too can be tricked at times. TLS is another identity verification tool which works the same as SSL but better than it. This provides some additional protection to the data so that no breaches are formed.

1: Differentiate a white box test from a black box test.
During a white box testing, the team that is responsible for performing the test is informed about the details related to it but in case of black box it's the opposite.

When black box testing is done, the testing team is not given any information and is rather kept in dark.

Q: What are the different ways in which the authentication of a person can be performed?
1. Passwords: This is something that the user should know from when they started their activity.
2. Token: This is something they are provided with and should have it.
3. Biometrics: This is an internal property of that person registered for verification.
OTP: A one-time pin or password is sent to the user through which they verify the identity.

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.

Top 50 Cyber Security Interview Questions and Answers (updated for 2018)

The interview process is tough, not only for the candidates but also for the interviewers. The process also depends on the position for which the hiring is done. For a replacement; the skills of the previous employee are taken as the benchmark. In case a team is getting expanded, the management knows the skills that they expect in the candidates. The interview process is tough because:

- Not many experienced professionals are there who are willing for a job change
- Interviewer expectations are always high from the candidates
- The right candidates don't fall in the budget cap.

Interviewers are usually interested in the candidates who have the necessary domain and technical knowledge unless they are hiring for a particular skill e.g. exploit development.

The Interview Process

- Resume shortlisting
- Basic HR questions
- Interview level 1 (Tech)
- Interview level 2 (Tech + Attitude)

Once the resume gets shortlisted, this gets followed by the basic HR call. This ensures that the resume is updated, the person is looking for a change and sometimes a basic set of questions

about your experience and reason for change. The call will also ensure that whether your resume has been sent for the next level review. The next level can be over a telephonic call, face to face interview or over Skype. Level 1 will actually test your knowledge whereas level 2 will go for your experience and attitude towards work. So be prepared with the basics of information security, technical knowledge and your resume well versed along with a positive attitude.

Different levels - Cyber Security Interview Questions & Answers

- **Level 01 - Basic Questions**
- **Level 02 - Learners (Experienced but still learning)**
- **Level 03 - Master (Entered into a managerial position or sitting for one)**
- **Level 04 - Grandmaster (Senior management roles)**

Level 01 - Basic questions (Not to be messed up)

1. Explain risk, vulnerability and threat?
TIP: A good way to start this answer is by explaining vulnerability, and threat and then risk. Back this up with an easy to understand example.

Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it.

2. What is the difference between Asymmetric and Symmetric encryption and which one is better?
TIP: Keep the answer simple as this is a vast topic.

Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption.

Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

3. What is an IPS and how does it differs from IDS?

IDS is an intrusion detection system whereas an IPS is an intrusion prevention system. IDS will just detect the intrusion and will leave the rest to the administrator for further action whereas an IPS will detect the intrusion and will take further action to prevent the intrusion. Another

difference is the positioning of the devices in the network. Although they work on the same basic concept but the placement is different.

4. What is XSS, how will you mitigate it?

Cross site scripting is a JavaScript vulnerability in the web applications. The easiest way to explain this is a case when a user enters a script in the client side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client side.

Countermeasures of XSS are input validation, implementing a CSP (Content security policy) etc.

TIP: Know the different types of XSS and how the countermeasures work.

5. What is the difference between encryption and hashing?
TIP: Keep the answer short and straight.

Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.

Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

6. Are you a coder/developer or know any coding languages?
TIP: You are not expected to be a PRO; understanding of the language will do the job.

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage - both in the interview and on the floor.

7. What is CSRF?

Cross Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples and countermeasures.

8. What is a Security Misconfiguration?

Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

9. What is a Black hat, white hat and Grey hat hacker?
TIP: Keep the answer simple.

Black hat hackers are those who hack without authority. White hat hackers are authorised to perform a hacking attempt under signed NDA. Grey hat hackers are white hat hackers which sometimes perform unauthorised activities.

10. What is a firewall?
TIP: Be simple with the answer, as this can get complex and lead to looped questions.

A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

11. How do you keep yourself updated with the information security news?
TIP: Just in case you haven't followed any: the hacker news, ThreatPost, Pentest mag etc.

Be sure to check and follow a few security forums so that you get regular updates on what is happening in the market and about the latest trends and incidents.

12. The world has recently been hit by ……. Attack/virus etc. What have you done to protect your organisation as a security professional?

Different organisations work in different ways, the ways to handle incident is different for all. Some take this seriously and some not. The answer to this should be the process to handle an incident. Align this with one you had and go on… just don't exaggerate.

13. CIA triangle?

- Confidentiality: Keeping the information secret.
- Integrity: Keeping the information unaltered.
- Availability: Information is available to the authorised parties at all times.

14. HIDS vs NIDS and which one is better and why?

HIDS is host intrusion detection system and NIDS is network intrusion detection system. Both the systems work on the similar lines. It's just that the placement in different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes processing power of the host as well.

Level 02 - Learners (Experienced but still learning)

15. What is port scanning?

Port scanning is process of sending messages in order to gather information about network, system etc. by analysing the response received.

16. What is the difference between VA and PT?

Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

17. What are the objects that should be included in a good penetration testing report?

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category wise split into high, medium and low. Also include detailed observation along with replication steps, screenshots of proof of concept along with the remediation.

18. What is compliance?

Abiding by a set of standards set by a government/Independent party/organisation. E.g. An industry which stores, processes or transmits Payment related information needs to be complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organisation complying with its own policies.

19. Tell us about your Personal achievements or certifications?

Keep this simple and relevant, getting a security certification can be one personal achievement. Explain how it started and what kept you motivated. How you feel now and what are your next steps.

20. Various response codes from a web application?

1xx - Informational responses
2xx - Success
3xx - Redirection
4xx - Client side error
5xx - Server side error

21. When do you use tracert/traceroute?

In case you can't ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc.

22. DDoS and its mitigation?

DDoS stands for distributed denial of service. When a network/server/application is flooded with large number of requests which it is not designed to handle making the server unavailable to the legitimate requests. The requests can come from different not related sources hence it is a distributed denial of service attack. It can be mitigated by analysing and filtering the traffic in the scrubbing centres. The scrubbing centres are centralized data cleansing station wherein the traffic to a website is analysed and the malicious traffic is removed.

23. What is a WAF and what are its types?
TIP: This topic is usually not asked in detail.

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

24. Explain the objects of Basic web architecture?
TIP: Different organisations follow different models and networks. BE GENERIC.

A basic web architecture should contain a front ending server, a web application server, a database server.

Level 03 - Master (Entered into a managerial position or sitting for one)

25. How often should Patch management be performed?

Patch should be managed as soon as it gets released. For windows – patches released every second Tuesday of the month by Microsoft. It should be applied to all machines not later than 1 month. Same is for network devices, patch as soon as it gets released. Follow a proper patch management process.

26. How do you govern various security objects?

Various security objects are governed with the help of KPI (Key Performance Indicators). Let us take the example of windows patch, agreed KPI can be 99%. It means that 99% of the PCs will have the latest or last month's patch. On similar lines various security objects can be managed.

27. How does a Process Audit go?

The first thing to do is to identify the scope of the audit followed by a document of the process. Study the document carefully and then identify the areas which you consider are weak. The company might have compensatory controls in place. Verify they are enough.

28. What is the difference between policies, processes and guidelines?

As security policy defines the security objectives and the security framework of an organisation. A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism. Guidelines are recommendations which can be customised and used in the creation of procedures.

29. How do you handle AntiVirus alerts?

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can

be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

30. What is a false positive and false negative in case of IDS?

When the device generated an alert for an intrusion which has actually not happened: this is false positive and if the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative.

31. Which one is more acceptable?

False positives are more acceptable. False negatives will lead to intrusions happening without getting noticed.

32. Software testing vs. penetration testing?

Software testing just focuses on the functionality of the software and not the security aspect. A penetration testing will help identify and address the security vulnerabilities.

33. What are your thoughts about Blue team and red team?

Red team is the attacker and blue team the defender. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

34. What is you preferred - Bug bounty or security testing?

Both are fine, just support your answer like Bug Bounty is decentralised, can identify rare bugs, large pool of testers etc.

35. Tell us about your Professional achievements/major projects?

This can be anything like setting up your own team and processes or a security practice you have implemented. Even if the achievement is not from a security domain just express it well.

36. 2 quick points on Web server hardening?
TIP: This is a strong topic, get over with the exact answer and carry on the conversation over the lines.

Web server hardening is filtering of unnecessary services running on various ports and removal of default test scripts from the servers. Although web server hardening is a lot more than this and usually organisations have a customised checklist for hardening the servers. Any server getting created has to be hardened and hardening has to be re-confirmed on a yearly basis. Even the hardening checklist has to be reviewed on a yearly basis for new add-ons.

37. What is data leakage? How will you detect and prevent it?

Data leak is when data gets out of the organisation in an unauthorised way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorised upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

Level 04 - Grandmaster (Senior management roles)

38. What are the different levels of data classification and why are they required?

Data needs to be segregated into various categories so that its severity can be defined, without this segregation a piece of information can be critical for one but not so critical for others. There can be various levels of data classification depending on organisation to organisation, in broader terms data can be classified into:

- Top secret – Its leakage can cause drastic effect to the organisation, e.g. trade secrets etc.
- Confidential – Internal to the company e.g. policy and processes.
- Public – Publically available, like newsletters etc.

39. In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?

Users are usually not provided with admin access to reduce the risk, but in certain cases the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only limited time post senior management approval and a valid business justification.

40. What are your views on usage of social media in office?
TIP: Keep an open mind with these kinds of questions.

Social media is acceptable, just ensure content filtering is enabled and uploading features are restricted. Read only mode is acceptable till the time it does not interfere with work.

41. What are the various ways by which the employees are made aware about information security policies and procedures?

There can be various ways in which this can be done:

- Employees should undergo mandatory information security training post joining the organisation. This should also be done on yearly basis, and this can be either a classroom session followed by a quiz or an online training.
- Sending out notifications on regular basis in the form of slides, one pagers etc. to ensure that the employees are kept aware.

42. In a situation where both Open source software and licensed software are available to get the job done. What should be preferred and why?
TIP: Think from a security perspective and not from the functionality point.

For an enterprise, it is better to go for the licensed version of the software as most of the software have an agreement clause that the software should be used for individual usage and not for commercial purpose. Plus, the licensed version is updated and easy to track in an organisation. It also helps the clients develop a confidence on the organisations' software and practices.

43. When should a security policy be revised?

There is no fixed time for reviewing the security policy but all this should be done at least once a year. Any changes made should be documented in the revision history of the document and versioning. In case there are any major changes the changes need to be notified to the users as well.

44. What all should be included in a CEO level report from a security standpoint?

A CEO level report should have not more than 2 pages:

1. A summarised picture of the state of security structure of the organisation.
2. Quantified risk and ALE (Annual Loss Expectancy) results along with countermeasures.

45. How do you report risks?

Risk can be reported but it needs to be assessed first. Risk assessment can be done in 2 ways: Quantitative analysis and qualitative analysis. This approach will cater to both technical and business guys. The business guy can see probable loss in numbers whereas the technical guys will see the impact and frequency. Depending on the audience, the risk can be assessed and reported.

46. What is an incident and how do you manage it?

Any event which leads to compromise of the security of an organisation is an incident. The incident process goes like this:

- Identification of the Incident
- Logging it (Details)
- Investigation and root cause analysis (RCA)
- Escalation or keeping the senior management/parties informed
- Remediation steps
- Closure report.

47. Is social media secure?
TIP: This is another debatable question but be generic.

Not sure if the data is secure or not but users can take steps from their end to ensure safety.

- Connect with trusted people
- Do not post/upload confidential information
- Never use the same username password for all accounts

48. Chain of custody?

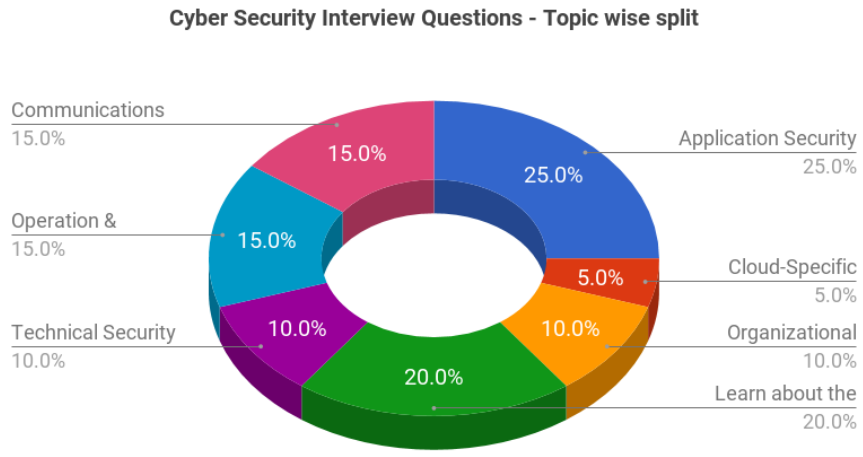
For legal cases the data/device (evidence) needs to be integrated, hence any access needs to be documented – who, what when and why. Compromise in this process can cause legal issues for the parties involved.

49. How should data archives be maintained?

Gone are the times when there used to be files and cabinets which held data over the years. This phase was long followed by archiving data over magnetic tapes and storing the tapes. There is another overhead for the maintenance and safety of the tapes. These are few conventional approaches, but the world is slightly moving to the cloud storage architecture. The only hurdle is the data privacy. Companies are not very sure about handing the critical data. This will actually take time but securely configured and managed cloud can be one of the best options.

50. What are your thoughts on BYOD?

There is no correct answer for this but just ensure that whatever side you are on, justify it with examples, scenarios and logic.



Although there is no defined scope and end to the questions, but having a strong foundation of the basic concepts and awareness about the latest trends will give you an upper hand in the interview.

TIP:

- **BACKUP** your answers with examples wherever possible.
- Provide **DETAILS**, this will leave less chance for the interviewer to dig into details.
- **BE PRECISE** in what you say, **LISTEN** carefully, **THINK** and **ANSWER**.
- **BE CONFIDENT** with what you speak.
- **MAINTAIN** a good posture.
- **BE AWARE** about the security news, recent incidents, attacks etc.
- Remember the question and answer accordingly, **DO NOT** get deviated from the topic.
- Most importantly "**KEEP A POSITIVE ATTITUDE**" even if the interview is not going as you expected.
- Sometimes it is kept that way to check the attitude.

Not to miss, to be in a top shape for your cyber security interview being a certified ethical hacker is an essential hiring criterion.