QUESTIONS & ANSWERS

F1. Why are you looking for a new position

An interviewer asking this wants to understand what has prompted a change in your career. Are you looking for more responsibility? A chance to expand your skill set? Do you feel that you outgrew your old position? Are you looking for more pay and less travel? Well then, why do you deserve more money and how are you more efficient working more from a central location? Explain your motivation for finding a new job in a way that shows that you view this new position as a positive change for both you and the organization.

2. What are your greatest strengths and accomplishments?

Take the opportunity to show how you helped your old company. Did you design its latest firewalls that prevented breaches? Did you re-route the routers? Help with information access security? Do you work well with people and show leadership skills? Talk about the types of technology you know well and how you made a positive impact in your last position. Explain how you built solid relationships with your coworkers and how you all worked together on successful projects—and how you intend to do the same at this new company.

3. What are your greatest weaknesses? (Related: How did you overcome a problem?)

Everyone makes mistakes, and no one is good at everything. You should honestly assess what you can improve and how you plan to show that improvement in your new role. Dig into your past: You might have overseen the response to a breach or some other serious problem. It might not have been your fault, but how you

handled it shows your professionalism, problem-solving abilities. and perhaps even outside-of-the-box thinking. Show that you are willing to learn from mistakes, even if they're not your own, and that you can handle a crisis. Explain how you took responsibility and stepped up to be a leader.

4. How do you envision your first 90 days on the job?

Your answer should encompass how you intend to meet with your team members to find out more about them and how you can work together. You should talk about how you will prioritize gaining an understanding of what your managers need from you and what all the stakeholders hope to achieve while also building strong rapport with your co-workers. You should ask what you can do to make an impact right away. Talk about how you intend to learn and get into the midst of business as soon as you can.

5. What is on your home network?

Your home network is typically a test environment. How you work with it gives an indication of what you would do with someone else's network.

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

Answering this question calls for a deep understanding of cyber security and anyone working in the field should be able to give a strong response. You should expect a follow-up question asking which of the three to focus more on. A simple way to put it: a threat is from someone targeting a vulnerability (or weakness) in the organization

that was not mitigated or taken care of since it was not properly identified as a risk.

7. How do you go about securing a server?

You might want to break this answer down into steps, especially if it refers to a specific type of server. Your answer will give a glimpse into your decision-making abilities and thought process. There are multiple ways to answer this question, just as there are multiple ways to secure a server. You might reference the concept of trust no one or the principle of least privilege. Let your expertise guide your response to this question and the others following it.

8. Why is DNS monitoring important?

Some argue that this is not necessary and that saying otherwise indicates that there are weaknesses in the domain name services. Others say DNS monitoring is prudent because DNS queries are a data-exfiltration vector from networks that allow any host to communicate to the Internet on Port 53.

9. What port does ping work over?

Watch out for this. Ping is a layer-3 protocol like IP; ports are an element of the layer-4 protocols TCP and UDP.

10. What is the difference between encoding, encrypting, and hashing?

This question should inspire a short conversation about encryption, which gives you the chance to explain your knowledge of it.

11. What is SSL?

SSL is a standard security technology for creating an encrypted link between a server and a client (usually a web server and a web browser).

12. What are the differences between HTTPS, SSL, and TLS?

HTTPS is hypertext transfer protocol and secures communications over a network. TLS is transport layer security and is a successor protocol to SSL. You have to demonstrate that you know the differences between the three and how network-related protocols are used to understand the inherent risks involved.

13. What sorts of anomalies would you look for to identify a compromised system?

There are multiple ways to answer this, but again, you need to show your expertise and ingenuity. One possible answer is drawing out a basic network architecture with its IPS/IDS, firewalls, and other security technologies to describe the type of traffic and other signs of compromise.

14. If you had to both compress and encrypt data during a transmission, which would you do first?

Compress and then encrypt, since encrypting first might make it hard to show compression having much of an effect.

15. How would you strengthen user authentication?

Whatever way you answer, mention two-factor authentication or non-repudiation and how you would implement it.

16. How would you defend against a cross-site scripting (XSS) attack?

Every cybersecurity professional should know this, even if it is difficult to answer. Come prepared with a thoughtful, concise plan for defending against this JavaScript vulnerability.

17. What are the differences between cybersecurity in the cloud and on premises?

Show that you understand the security risks inherent to both and which might be more appropriate for the company.

18. What does RDP stand for?

Remote desktop protocol, and its port number is 3389.

19. What is the difference between symmetric and asymmetric encryption?

Symmetric encryption uses the same key to encrypt and decrypt, while asymmetric encryption uses different keys for encryption and decryption. Asymmetric encryption is commonly used to secure an initial key-sharing conversation, but then the actual conversation is secured using symmetric crypto. Communication using symmetric crypto is usually faster due to the slightly simpler math involved in the encryption/decryption process and because the session setup doesn't involve PKI certificate checking."

20. What is the difference between UDP and TCP?

Both are protocols for sending packets of information over the internet and are built on top of the internet protocol. TCP stands for transmission control protocol and is more

commonly used. It numbers the packets it sends to guarantee that the recipient receives them. UDP stands for user datagram protocol. While it operates similarly to TCP, it does not use TCP's error-checking abilities, which speeds up the process, but makes it less reliable.

21. What is a trace route?

A traceroute, or tracert, can help you see where a breakdown of communications occurred. It shows what routers you touch as you move along to your final destination. If there is somewhere you cannot connect, you can see where it happened.

22. What tech blogs do you follow?

Show that you stay current by telling the interviewer how you get your cyber security news. These days, there are blogs for everything, but you might also have news sites, newsletters, and books that you can reference.

23. What do you do in your spare time outside of cybersecurity?

The interviewer is hoping to get a better sense of you as a person to determine whether you're trustworthy, reliable, and of good character. He or she also wants to see if you would be a good culture fit and someone others would enjoy collaborating with. You don't need to get too personal with the details, but you can talk about your hobbies, your family, the last vacation you took, or how often you like to work out, among other things. Show some personality here.

24. Where do you see yourself in five years?

Most people expect to advance in their cybersecurity careers in five years, which could mean a promotion or raise (or a few). Emphasize how you are looking to further your knowledge and skills—and how that will benefit the company. Tell the interviewer that you see yourself moving up to a more senior position and continuing to contribute to the organization in a significant way. Drive home the point that the investment made in you will be a good one.

25. Do you have any questions?

This is your chance to find out more about the company and position. Remember that an interview is a two-way street. You are interviewing them as much as they are interviewing you (even though it doesn't always feel that way). Ask about the work environment and what the company expects of you. Find out more about the day-to-day responsibilities and whether there any special projects on the horizon. And see if you and the company are a good fit culture-wise.

****

26. Explain risk, vulnerability and threat?

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.

27. 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.

28. 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.

29. 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.

30. What is the difference between encryption and hashing?

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.

31. Are you a coder/developer or know any coding languages?

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.

32. 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.

33. What is a Security Misconfiguration?

Security misconfiguration is 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.

34. What is a Black hat, white hat and Grey hat hacker?

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.

35. What is a firewall?

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.

36. How do you keep yourself updated with the information security news?

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.

37. 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.

38. CIA triangle?

Confidentiality: Keeping the information secret.

Integrity: Keeping the information unaltered.

Availability: Information is available to the authorised parties at all times.

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. Various response codes from a web application?

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

46. 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.

47. 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.

48. What is a WAF and what are its types?

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.

49. Explain the objects of Basic web architecture?

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

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. Which one is more acceptable?

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

56. 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.

57. 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.

58. 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.

59. 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.

60. 2 quick points on Web server hardening?

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.

61. 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.

62. 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.

63. 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.

64. What are your views on usage of social media in office?

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.

65. 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.

66. In a situation where both Open source software and licensed software are available to get the job done. What should be preferred and why?

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.

67. 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.

68. 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.

69. Is social media secure?

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

70. 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.

71. 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.

72. 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.

73. 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

74) 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

75) 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

76) 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.

77) 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

78) 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.

79) List out various WEP cracking tools?

Various tools used for WEP cracking are

Aircrack

WEPCrack

Kismet

WebDecrypt

80) 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

81) 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

82) 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

83) 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

84) 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.

85. 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**

86. 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.

87. 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.

88. 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 authorised 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.

89. 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.

90. 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.

91. Strike the difference between vulnerability, a risk and a threat?

QUESTIONS & ANSWERS

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.

92. 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.

93. 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 defence mechanism and also can track down new vulnerabilities.

94. 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.

95. 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.

96. 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.

97. 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.

98. 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 memorise their IP address.

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

104. 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.

105. 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.

106. 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.

107. 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.

108. 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.

109. 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.

108. 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.

109. 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.

110. 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.

111. 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.

112. How to prevent identity thefts?

Identity theft refers to the acquisition of personal data of the victim and uses it for illegal purposes. It is the most common type of fraud that may lead to financial losses and at times may be held responsible for criminal actions as the victim might be personified.

A few of steps to follow in order to prevent identity thefts include:

Ensure the strong and unique password

Avoid postings of confidential information online

Do not post personal information on social media

Shop from known and trusted websites

Use the latest version of the browsers

Install advanced malware and spyware tools

Use specialized security solutions against financial data

Always update your system and the software

Protect the social security number

Download only the well-known apps and share limited details

113. What is a Security Mis configuration?

Security mis configuration 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

114. Information Security? Why?

A standard question type. All we're looking for here is to see if they pay attention to the industry leaders, and to possibly glean some more insight into how they approach security. If they name a bunch of hackers/criminals that'll tell you one thing, and if they name a few of the pioneers that'll say another. If they don't know anyone in Security,

we'll consider closely what position you're hiring them for. Hopefully it isn't a senior position.

115. 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

116. 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.

117. What is the protocol that broadcast the messages across all the devices?

Internet Group Management Protocol [IGMP] is the communication protocol which is used in video or game streaming. This communication protocol facilitates the

communication devices and the adjacent routers to send packets across the network

118. What are the risks if I use public Wi-Fi?

It is the general tendency of the public to prefer Wi-Fi in spite of having independent data plans as it is faster and free.

However, Wi-Fi comes with certain security issues. A few of the public Wi-Fi attack includes brute-force attacks, war-driving, sniffing, karma attack, and, etc. it would definitely obstruct the data that is conveyed through the router like the passwords, emails, addresses, credit card data, browsing history, and, etc.

This could be minimized by using routers that are encrypted with WPA2 alone.

And, when connected to public Wi-Fi it is suggested to take the following steps.

Turn-off the public networking sharing of the data.

Enable the firewall at all times

Use only the secure websites for sensitive operations.

Encrypt the IP address by using the Virtual Private Network [VPN].

Do not forget to turn-off the Wi-Fi once work is done.

Keep your system always updated to latest version and patch-up.

Keep your system free of malware by using the latest and reliable antivirus.

Browse the sites only with a good anti-spyware solution[s].

Avoid any kind of financial transactions on public Wi-Fi unprotected.

Ensure you have the latest browser with the security patches.

Use the two-factor authentication factor as an extra security measure.

119. 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.

120. 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.

121. 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 authorised 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.

112. Is social media secure?

The online social sites like the Facebook, Twitter, LinkedIn, Instagram, and so forth are becoming more agreeable for networking, business communications, and professional benefits creating a major and direct impact of our life activities.

Though the extent of networking is favorable and appreciated, it is creating space for intruders too. As we find headlines about data breach through social media, the use of social networking is getting reconsidered.

Recommended for You Back to Basics: Top 5 Social Media Safety Tips

However, there are measures to stay safe on social media. The possible risks are hacking, identity theft, bullying, standing, damage reputation, impersonators, and, etc.

A few of the measures to follow includes:

Avoidance of sharing personal things

Limiting the details about work in LinkedIn

Screening of images or any personal news before posting

Educating oneself about the rules followed in social postings

Connect with only trusted people

Have stronger and unique passwords for different social channels

It is recommended to be generic on social media

And more

113. 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.(Cobit 5 Training)

114. 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.

115. What is a Firewall?

A firewall is a device placed on the boundary of the trusted and untrusted networks. One can set or define the rules that allow or blocks the traffic accordingly.(Cyber Security Interview Questions)

116. What's the difference between HTTP and HTML?

Obviously the answer is that one is the networking/application protocol and the other is the markup language, but again, the main thing you're looking for is for them not to panic. The object here should be identifying absolute beginners and/or having fun with people who know how silly the question is.

117. What's the goal of information security within an organization?

This is a big one. What I look for is one of two approaches; the first is the über-lockdown approach, i.e. "To control access to information as much as possible, sir!" While admirable, this again shows a bit of immaturity. Not really in a bad way, just not quite what I'm looking for. A much

better answer in my view is something along the lines of, "To help the organization succeed."

This type of response shows that the individual understands that business is there to make money, and that we are there to help them do that. It is this sort of perspective that I think represents the highest level of security understanding—-a realization that security is there for the company and not the other way around.(The Best Blockchain Interview Questions And Answers (Updated 2018))

118. Why do you want to work as an incident responder?

Questions like this can sometimes come as a surprise in an interview, especially if you were getting ready to dazzle the interviewers with technical answers and not general ones like this. This is a great opportunity for you to spell out your career path so far and how your experiences in previous roles led you to where you are now.

Don't be afraid to highlight some of your achievements, either. The interviewers will be looking at what kind of work you have done that actually fits in with the role you have applied for. Keep your answers relevant to the role and don't go off on too much of an unrelated tangent.

119. What do you think that this role requires from you?

This question could be asked in just about any interview and is by no means an incident responder-specific question, but it is definitely one that needs a careful answer. Your interviewers are looking to find out if you have the right expectations of the work you are going to do, and what the role actually requires from you.

Be sure to mention that incident response requires quick and careful actions, as you are normally the first person to work on the problem. Mention that you look at resolving the issue as quickly as possible while minimizing further damage, but that you are just as concerned with documenting the circumstances around the failure for later analysis and inspection.

120. How would you handle an outage on operation-critical systems such as data links between sites?

The first thing to check is that the backup link is fully functional and that business operations are working as expected. Tell them that the multiple systems that need to communicate must all be checked, and that it is business as usual for your applications and services. Once the extent of the affected service's impact has been quickly assessed, you can proceed with the actual investigation and incident response into getting the service back up and running.

Mention that you would test the link, check that the hardware is responding and that the line services were active. If it is found to be hardware-related, then the

correct teams would be dispatched as necessary. If it is a service provider that is offline, then you would coordinate with them to resolve the issue as quickly as possible.

121. What kind of security breaches would you be on the lookout for?

This question seeks to test your knowledge of cybersecurity-related breaches, so think of the most common ones that you are likely to deal with.

One common example is SQL injection. Mention how it runs on a server, and how an attacker can use it to run other commands through this exploit that could potentially give them further access to the network. You might also mention man-in-the-middle attacks, DDoS, or cross-site scripting as well. Just make sure that you brush up on your explanations before your interview.

122. Why would you check file changes on a system, and how would you compare them?

There are a few reasons why files might have changed in unexpected ways, especially if you are not aware of any legitimate processes running on the target machine. You can mention that malware, viruses or unauthorized access all have the potential to cause changes in files.

Mention that using an MD5 hash is one of the most common ways to show that a file has changed, especially

since the metadata of a file (which includes access and creation data, as well as ownership) can be edited by malicious code or a skilled intruder.

123. What document would you need to restore a system that has failed?

The correct document to look for when recovering from a serious system failure would be a disaster recovery document. This document outlines all of the steps and considerations that you should take when looking to restore a failed system.

124. What is port scanning and why would you use it?

Port scanning is a process that scans a computer or server and checks to see what communications ports are currently open, closed or active. Many network protocols use a designated port number in order to communicate, so looking at open ports will give an incident responder clues about the applications that are running in the background.

Port scanners are used in situations where the incident responder is trying to troubleshoot why an application is not working as expected, or as a means to test if there are unauthorized connections to a server or computer. Port scanners are commonly used and give incident responders a greater view of the network state.

125.Are you a team player or do you prefer to work alone?

For junior positions, it is almost always the case that you will be joining a team of other incident responders and cybersecurity professionals. The chances are high that you will be required to fit into an existing team, so showing your willingness to cooperate with others will go a long way to help show that you are suitable for the role.

Don't be afraid to let the interviewers know that you are also perfectly happy to work on your own when required, as there are projects that get given out in any position that will sometimes only require one person to work on it.

126. What is a cybersecurity incident?

Being able to explain what you consider an incident is very important, because you are the one that is responsible for responding to them as certain conditions are met. You shouldn't need to give an overly-detailed response, just a clear and concise explanation.

You could think of an incident as something like a breach in a system's safety measures and security policy that either brings a system down or affects the way that it operates in a negative way. Another way to classify a cybersecurity incident is as unauthorized access or attempts to access a system or to the data of a system, such as a hacking occurrence or an attempted hack.

127. How do you decide how to respond to a given scenario?

There are a few ways that you could answer this question, because it is very open-ended. The truth is that it's probably there so that the interviewers can see how you would react in a given situation.

Be sure to mention that the Incident Response Policy would be the main guide for how you would conduct the incident response activity, and that your actions would fall in line with the best practices of the organization.

128.What are HIDS and NIDS?

As a more senior incident responder, you will be familiar with different kinds of detection systems and which ones are used in specific scenarios. You should know that a Host Intrusion Detection System (HIDS) runs on servers and computers, while a Network Intrusion Detection System sifts through network traffic and sniffs out anomalies and other suspicious behavior.

129.What is Automated Incident Response?

Automated Incident Response systems help to reduce the time taken by engineers to identify a threat and isolate it by performing automated tasks that would normally take

a long time to complete. These examples include log file analysis and collating data from seemingly-disparate and unrelated sources. These technologies are becoming more common, so having some knowledge of how they work will be a plus in the interview.

130.What is SIEM?

Any incident responder worth their salt knows what a Security Information and Event Management system is, so this question should be a no-brainer if it comes up in the interview. All a SIEM does is aggregate data from multiple sources and compile them into meaningful information. Depending on the software, they can also detect potential or ongoing threats and block access, depending on how the environment has been configured and how the rules have been set up. Showing basic SIEM knowledge is essential for this level of interview, so be sure to brush up on your knowledge ahead of time.

How would you detect incoming threats?

First, you would identify that suspicious or strange activity has been confirmed via the SIEM or through other sources such as firewall logs or alerts. Once confirmed, you then outline the basic steps of checking logs and documenting your findings as you progress. Specify that the Incident Response Policy document would dictate the proper response, as well as the correct escalation procedures. It is important to show the interviewers that you understand that the role of an incident responder is to act in concert with the team, and not to go off on a solo

investigation without informing everybody else about a potential threat.

How do you stay up-to-date with the latest information security developments relating to incident response?

Feel free to share the different sources that you use with the interviewers. Think about the different forensic/information security resources such as blogs, forums, newsletters and social media sources that you lean on when you are researching or learning about new threats. Be sure to put across the fact that you are always looking to learn more and evolve professionally.

131.What operating systems are you familiar with?

At this level, you should ideally be proficient in Windows and Linux/Unix environments. Some organizations have a mix of different operating systems, and knowledge of how these systems are vulnerable to exploits is really important. Each operating system stores information in different ways, and log files are stored differently as well. Make sure that you are honest about your proficiency (or lack thereof) early on so that there are no false expectations.

How important are system-wide security and vulnerability assessments?

Vulnerability assessments are an ongoing process that never ends, which is why there are usually daily, weekly and monthly checks that need to be done across the different systems within an organization. Most of these

checks are done via the SIEM, but some need to be checked manually. Researching issues and staying current with news and updates is essential if you are going to keep up with malware and hacking developments.

How important are documentation and procedural responses?

The interviewers are looking to see if you understand how important the procedures and documentation steps of the organization are. Be sure to mention how procedures need to be updated, and that each document must keep a version number to show when last the document or procedure was updated or revised. Document contributors and authors must also be acknowledged so that the document history is properly managed and understood. Explain that the procedural responses are vital because they determine how each scenario is dealt with.

132.What are some of the steps that you take after an incident?

This process goes by many different names: postmortem, root cause analysis, learning review, post-incident review and more. You can give a brief outline of the kinds of information that you normally include in such reports, like the services that went down, who they affected, how long the downtime was experienced, who helped with the response and how the issue was eventually fixed.

Preventative actions are also a part of post-incident reports, so be sure to mention that the best way to prevent

such things from reoccurring is to show what worked in the response plan and what didn't. The response plan can then be updated accordingly.

133.What are some of your professional achievements or major projects that you completed?

This is your time to dig deep and think about all of the impressive things that you have accomplished over the years. Perhaps you were tasked with researching a solution to a new threat, or maybe you were the response lead during an incident — anything that highlights your strengths will show the interviewers that you have what it takes to fill the role.

134. What is a pentest and what processes would you include?

Pentesting is a skill that you will need to have in your arsenal if you are hoping to get to this level of incident response. Not only is it important for understanding how an attacker is getting through your defenses in times of an active incident, but it is also really important for postmortem briefs where you will need to recreate the incident with similar techniques to the attacker.

The answer to the question is very open-ended, so expect more specific protocol-related derivatives of this line of questioning. The interviewer will probably paint a picture of a specific incident where certain behaviors are detected

on your monitoring setup, requiring you to investigate. Be prepared to describe the tools and uses that each of them is needed for, as well as some personal experiences of how you have leveraged your pentesting abilities in the past to thwart an attack or investigate the aftermath of such an attack.

135.What pentesting methods are there, and which are you familiar with?

You probably won't need to recall all of these methods verbatim, but any experience that you have with each one will be a plus. The most common pentesting methods are external testing, blind testing, double-blind testing, and targeted internal testing. If you have experience with any of these, great. If not, then make sure you let them know which ones you are most proficient with.

136.How would you describe your communication style?

Communication at this level of incident response is critical if you are going to be leading a team of people, especially during a crisis. The interviewer is looking to find out how you deal with communication between yourself and the different departments in the organization, such as Human Resources, Legal and the C-suite executives.

Equally important is your communication skills with your team as you will be driving communication and action from each of them, and in some cases across multiple

regions. You might have to elaborate on your cultural understanding between countries if you are going to head up a multinational response team for larger organizations. The key thing to show is that you can communicate well and that you understand who needs to be informed and updated, all while you drive the threat response.

137.What incident response team-based events have you overseen or participated in, and what did you learn?

This is a good chance for you to speak about some of your past experiences either as a team member or team leader. Talk about the problems you faced and the techniques that were used when trying to isolate the problem. Be sure to mention the different phases of your response, such as containment, preservation, eradication, recovery and postmortem. Explain what you need to do for each step, and how past incidents that you were part of were broken down into each of these different phases.

138.What are some mistakes that you have made in the past? How did you learn from them?

This is a good place to be honest about some of the errors you might have made earlier in your career, or a simple mistake from just last week: You need to decide how relevant the example is that you are giving to the interviewers.

Obviously, you don't want to paint yourself as being reckless or incompetent, so keep things limited to mistakes that you made where you were able to learn from and rectify the situation. Perhaps you once locked yourself out of an appliance such as a router or network switch, or lost comms to a device after making a bad configuration change.

Explain how you worked around the problem and then made sure that you didn't let it happen again. Interviewers are looking for honesty here, so be sincere and think about some of the learning experiences that you have had over the years and have one or two examples ready for them.

139.What is a cross-site scripting attack?

This is a big talking point, as the vulnerability has been exploited by hackers for quite some time already. Make sure that you are familiar with all of the basic elements that make up an attack of this nature ahead of time, and make sure that you can explain what the attack is so that it makes sense even to the non-technical people that may be sitting in on the interview.

Make sure that you explain the essence of the attack, showing that you understand it properly. Mention how it is a client-side attack that injects malicious scripts and code where the script is interpreted and run by the server. This allows the attacker to gain access to the machine or to inflict damage via a malicious payload. We went through a few of these in this article here, so take a look before your

interview and brush up if you need a refresher on any of the finer details of this and other web app vulnerabilities.

140.You've been given the chance to build your own CSIRT. What would you need?

This is a fun question to answer, as it is quite open-ended. Roles that require managerial and planning experience might want to see how you envision the role of the CSIRT (Computer Security Incident Response Team) within an organization. The answers that you give will depend on the size of the organization, the budget for the team, how the department fits in with the SOC (Security Operation Center) and CERT (Community Emergency Response Team), and if there are any overlapping responsibilities between the teams. You can also make suggestions for threat intelligence systems and other tools that you would recommend.

141.What is an APT and how would you effectively deal with one?

Advanced Persistent Threats are usually groups of cybercriminals that gain access to a network and remain hidden while stealing information or jeopardizing systems. Traditionally this was the work of state-sponsored cyber-divisions that would attack international targets, but this has become a more localized threat in recent years. The availability of tools and the growing number of skilled attackers has made these types of incidents far

more common than they were before, though they are still relatively rare.

Dealing with this kind of threat requires an intelligent threat response system in conjunction with a team of threat hunters to actively and routinely investigate the environment for suspicious behavior and anomalies in the system logs. Proper security audits must be carried out routinely to establish if any intrusion attempts have been made, whether successful or not.

142.Tell us about the most difficult incident that you have ever had to respond to.

This kind of question lets you sculpt the answer to fit the narrative of the interview up to this point, because you would have an idea of the requirements of the role. Draw from your past experiences and mention something that relates to some earlier questions, and don't be afraid of going into details about the processes that you followed, as well as the outcomes. This is a great opportunity for you to showcase the skills that you have, and how they would be applicable to the company that is interviewing you.

142.How do you deal with a technical situation that you cannot figure out on your own?

There is no shortage of potential incident response resources, both internal and on the Internet. The first port of call would be your internal playbook and policy guides.

These would assist with determining the next course of action given a specific set of failures and outcomes.

Next would be policy frameworks and your department's incident response plan. Failing that, you could lean on other members in your department that have more direct experience with a specific threat, or if it seems to be more of a specialized issue, then you could look at collaborating with another department to get to the bottom of the problem.

You want to show both your willingness to get your hands dirty tackling the problem while showing restraint with regards to spending too much time on a bad solution. Time is critical in this line of work, so you want to make sure that you are able to walk that fine line between the two approaches.

143.Bonus Tip: Learn as much about the company as you can prior to the interview

Learn and figure out as much as you can about the company that you are interviewing for ahead of your appointment for the interview and find out about what their key business is. Think logically about what services they would have and try to reasonably assess what their key security concerns might be. This will help you to look like a much better candidate when asked any company-specific questions that could potentially come up as you will be showing keen interest in the organization, which always impresses a potential employer.

Conclusion

QUESTIONS & ANSWERS