Entry Level Cybersecurity Interview Questions

By Surendra Pander {@technical surendra}

Cyber Security Interview Questions - Software and Programming

This section will take you through a set of cyber security interview questions based on software and programming.

11. How do you keep your computer secure?

There are a few steps that one has to implement in order to keep their computer secure. A few of these steps are :

1. Implement a 2-way or multi-factor authentication
2. Use uncommon alphanumeric passwords and secure them
3. Update your computer regularly
4. Install a good antivirus to protect your computer from malware
5. Have a specialized firewall to keep attacks at a minimum
6. Have anti-phishing software installed to identify fraudulent mails
7. Use encryption to reduce data leakage and loss
8. Finally, it is very crucial to secure your DNS

12. Discuss security-related aspects between C, C++, and Java.

Aspects	C	C++	Java
Pointers	Supports pointers, most secure.	Supports pointers, secure.	Not supported, direct access to the memory location.
Code translations	Compiled, not secure.	Compiled, not secure.	Interpreted, abstracted, and secure.
Storage allocation	Uses malloc, calloc, less secure.	Uses new, delete, comparatively secure.	Uses garbage collector, more secure.

Inheritance	No inheritance, not secure.	Supported, most secure.	Multi-inheritance not supported, comparatively secure.
Overall	Least secure	More secure	Most secure

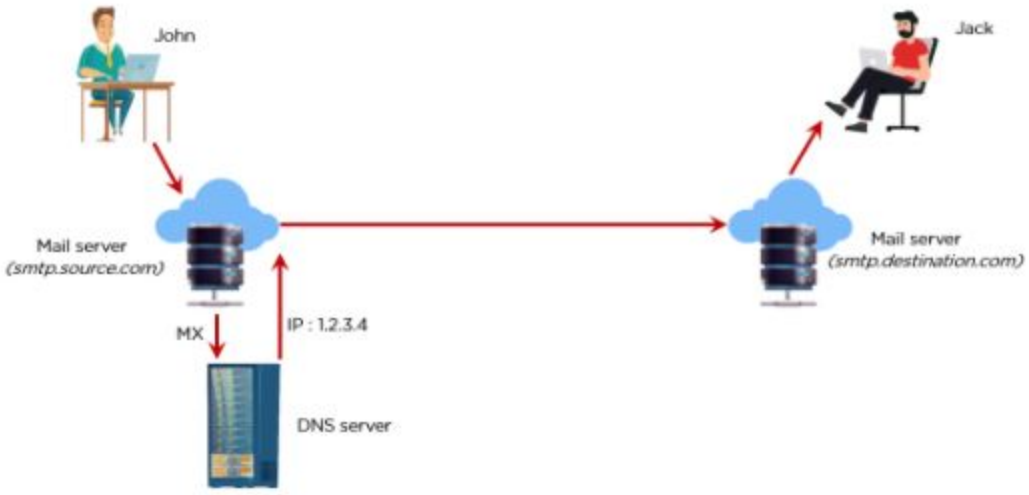
13. What are the different sources of malware?

Malware is a malicious software that harms the security of your device. The different sources of malware are:

1. Pop-ups
2. Removable media
3. Documents and executable files
4. Internet downloads
5. Network connections
6. Email attachments
7. Malicious advertisements

14. How does email work?

As you can see below, here, there are two servers, both using SMTP. We have John and Jack, and in this scenario, John wants to send an email to Jack. Thus, they have an email client installed on their machine connected to the mail exchange server, which has a DNS server that maps the routing and maps the exchange server and inboxes.



So when John composes the message and clicks on send, he should be connected to a mail exchange server where the email is sent through that particular person's inbox. So John's inbox will then be validated, and that email will then be sent through the DNS server through the internet and will be received by the recipient mail server.

While John composes the mail, the from the field will have his email address, and the to the field will have Jack's email address. When he clicks on send, it will go to their exchange server. The exchange server will then validate the inbox and identify where the inbox is located for Jack, and then through the internet, it will be sent to the mail server of Jack.

The mail server will then identify the right inbox that email needs to be sent to, and it stores the email in that particular inbox of the recipient. This way, when Jack accesses his inbox, the email from John will be waiting in his inbox. Jack can then reply the same way John sent the email.

15. What are the types of threats a company can face?

There are several threats that a company can face; on a broader scale, we can classify them as:

1. Natural Threats: These include natural disasters beyond human control, threats like a tornado, fire, floods, etc.
2. Man-made: These are threats where humans are the cause, like theft, hacking, etc.
3. Technical: These threats could be either a software bug or a server fail, or any technical failure.
4. Supply System: Any electric outage or short circuit kind of problem falls under this category.

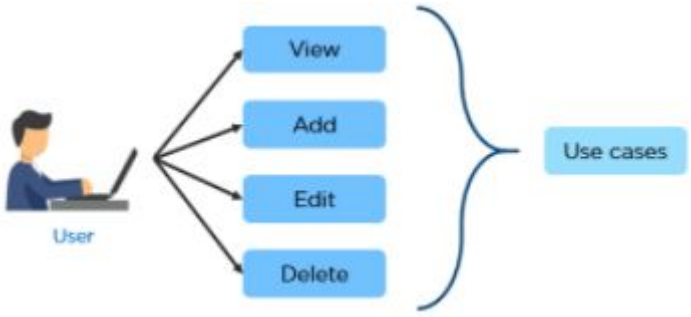
16. What are black box and white box testing?

In black box testing, the tester has zero knowledge of the IT infrastructure. Here, the testers will be unaware of the application, and they would have to gather information all by themselves. Based on the gathered information, testers will identify system vulnerabilities, if any. It is important as it emulates the attack of an external hacker.

A white box attack emulates an insider who can be an employee in the organization trying to make unvalidated profits. In this form of testing, the tester has complete knowledge of the IT infrastructure.

17. What is use-case testing?

Use-case testing is a functional black box testing. Testers use it to get the test scenarios to exercise the entire system from start to finish. For example, when the software is made for users to use for documentation. The testers will test all the cases that a user can do like shown below:



18. What is static and dynamic testing?

Static Testing	Dynamic Testing

Static testing is done in the early stage of the development life cycle.	Dynamic testing is done at the end of the development life cycle.
It includes walkthroughs and code review.	It includes functional and non-functional testing.
Static testing is 100% accurate in a very short amount of time.	Dynamic testing involves several test cases that take a longer time.
Static testing is about prevention.	Whereas dynamic testing is about a cure.

19. What are the test levels in software testing?

The test levels in software testing are:

1. Module testing: It checks subprograms, procedures, routines, and subroutines in a program.
2. Integration testing: Here, the combined parts of an application of software are tested to check if they function correctly or not.

3. System testing: System testing tests the entire system or software or any application.
4. Acceptance testing: The quality assurance team does this testing to check if the clients' requirements are met or not.

20. What are the valuable steps to resolve issues while testing?

The following steps can be implemented to resolve issues while testing:

1. Record: Log and resolve the problems which have happened
2. Report: Report issues to the higher-level managers
3. Control: Define the issue management process

Let's now proceed to the next section of this article on cybersecurity interview questions.

21. What is the difference between Symmetric and Asymmetric encryption?

Basis of Comparison	Symmetric Encryption	Asymmetric Encryption
Encryption key	ONE Key for ● Encryption ● Decryption	TWO keys - ● One for encryption ● One for decryption
Performance	● Fast Encryption ● Higher risks	Slow Encryption for high computation

Algorithms	• DES • 3DES • AES • RC4	• Diffie-Hellman • RSA
Purpose	Best in bulk data transmission	Preferred for secure exchange of secret keys

22. What is the difference between IDS and IPS?

- Intrusion Detection System (IDS) - performs only one action
    - Detects intrusions, and
    - Administrator should handle prevention of intrusion
- Intrusion Prevention System(IPS) - performs two actions
    - Detects intrusion, and
    - Prevents intrusion

23. Explain the CIA triad.

A key set of guidelines used by most organizations for securing information is called the CIA Triad: Confidentiality, Integrity, and Availability.

- Confidentiality: Accessible and readable only by authorized personnel.
- Integrity: Data is not manipulated by unauthorized personnel.
- Availability: Ensuring data is available to the user whenever it is required. It should also support hardware maintenance, regular upgrades, recovery, network bottleneck, and data backup.

24. How is Encryption different from Hashing?

Encryption and Hashing convert data in readable format into an unreadable format. In the case of encryption, data CAN BE converted into its original form by decryption. However, in the case of hashing, data CAN NOT be returned to the original format.

25. What is the difference between VA (Vulnerability Assessment) and PT(Penetration Testing)?

Vulnerability Assessment:

This is the process deployed to find out the flaws in the target itself. This is because the organization has already determined the flaws or weaknesses and has to prioritize the issues for fixing.

Penetration Testing:

In this method, the attempt is to find the vulnerability of the target itself. The process is to establish if the security measures the organization has implemented are sufficient to protect it from being hacked and if the system and network are well protected.

26. What is a three-way handshake?

An important method deployed in TCP/IP networks is the three-way handshake. It creates a connection between the client, and the host and follows three steps and hence the name.

1. One, the client first sends an SYN synchronization packet to the server to check if the server has open ports.
2. Two, the server will then send an SYN-ACK packet to the client if its ports are open.
3. Three, the client will acknowledge and reply and send an ACK packet back to the server.

27. What are the response codes that can be received from a Web Application?

There are response codes that are received from a web application. They are as follows:

- 1XX is information responses
- 2XX is success
- 3XX is redirection
- 4XX is client-side error

- 5 XX is server-side error

28. What is traceroute? Why is it used?

The use of a traceroute is to identify the path of a packet. It provides the points, especially the main nodes that the packet will pass through. The main purpose of using a packet is to identify when a packet does not reach a destination. The traceroute tool is used for evaluating the connection stops and the breaks at any point of failure.

29. What is the difference between HIDS and NIDS?

There is one main difference between HIDS and NIDS. At the macro level, HIDS for Host IDs and Network ID is an intrusion detection system and focuses on identifying any attacks. At the micro level, the basic difference is in how the Host IDS is established on the host or the device. It will monitor the traffic for that particular device every time there is suspicious activity. But NIDS is established for the entire network. It will monitor the traffic arising from every device on the network.

30. What are the steps to set up a firewall?

There are several steps followed to set up a firewall. They are:

1. Password and username: The default password for the firewall device is modified.
2. Remote administration: Disabling the remote administration feature.
3. Port forwarding: The appropriate port forwarding is configured for certain applications to perform correctly. For example, a web server or FTP server has to be configured to the appropriate port.
4. DHCP server: When there is an existing DHCP server, installing the firework will lead to conflict. Only, when the firewall HCP is disabled will it work.
5. Logging: Troubleshooting firewalls and protecting against potential attacks login is enabled to understand the nature of logins or view the logs.
6. Policies: The organization should implement well-structured security policies to ensure that users and external users follow the required protocol and ensure that the firewall is configured to follow through with the established policies of the organization.

31. Explain SSL Encryption

Secure Sockets Layer (SSL) is the standard followed in the security knowledge industry to develop encrypted connections between the browser as well as the web server. This standard ensures that data privacy is maintained and that online transactions are protected from external attacks.

The following steps have to be followed to establish an SSL connection:

1. The browser will connect to the web server which is secured by SSL.
2. The browser will send a copy of the SSL certificate.
3. The browser verifies if the SSL certificate is trustworthy. If trustworthy, the browser will send a message to the server requesting to establish an encrypted connection.
4. The web server acknowledges and starts to build an SSL encrypted connection.
5. The encrypted SSL communication begins between the browser and the web server.

32. What steps will you take to secure a server?

The Secure Socket Layer (SSL) is a protocol where data encryption and decryption will protect it from being intercepted by authorized users. The simple ways to secure the server are as follows:

1. Ensure that the password for root and administrative users is secured.
2. New users can be included in the system now. They will manage the system as per the policies established.
3. Remote access is removed for default administrator accounts.
4. The following steps have to be followed to configure Firewall rules for remote access.

33. Explain Data Leakage.

Data leakage is defined as the unintentional or planned leakage of data of an organization to external users, those who do not have permission to access or view such data. It typically is the disclosure of confidential information to unauthorized users. There are three ways in which such leakage can occur:1.Accidental Breach: A user has unintentionally sent the data to a person who is not permitted to view it and is thus a personal error or blunder.2. Intentional Breach: A user sends confidential data to an entity that is not permitted to view it, on purpose.3. System Hack: Different techniques are used such that data leakage is triggered. The major solution to contain data leakage is to use preventive tools software and certain techniques or strategies called the data leakage prevention tools.

34. What are some of the common Cyber Attacks?

Some of the common types of cyber attacks are Phishing, password attacks, malware, drive-by downloads, man-in-the-middle, roque software, and malvertising.

35. What is a Brute Force Attack? How can you prevent it?

Brute force is the attempt to repetitively try different permutations and combinations to break a given password. There are automated tools and software that try to login based on a list of credentials.

36. What is Port Scanning?

Port scanning is defined as the method to identify ports that are open and use the services of the host.

37. What do you understand about "Risk, Vulnerability & Threat" in a network?

- Threat is defined as the potential harm to a system or organization by a likely attacker.
- Vulnerability is defined as the weakness in the system which the hacker can exploit.
- Risk is the loss or damage that is likely to happen when the Threat will attack a Vulnerability.

38. How can identity theft be prevented?

Identity theft can be prevented by ensuring unique passwords, social media restrictions, shopping from trusted websites, installing spyware and malware protection tools, using only specialized security solutions for financial data, and always updating systems and software.

39. How often should you perform Patch management?

Patch management has to be applied as soon as they are released. The purpose of a patch is to overcome existing vulnerabilities in a system. Any delays in the patch update would only result in exposing the system to risks and attacks.

40. How would you reset a password-protected BIOS configuration?

BIOS is a pre-boot system and influences its own storage mechanism for references and other settings. It is reset by popping the CMOS battery out so that the settings in the memory are discharged and new settings can be installed after the battery is replaced.

41. Explain MITM attack and how to prevent it.

MITM attack or a man-in-the-middle attack is a severe type of Cyber attack since the hacker will remain between the communication of two parties and steal all information. The data from both parties are used by the hacker to redirect the data to a third destination party leaving both parties compromised.

42. Explain DDOS attack and how to prevent it.

Distributed denial of service attack is one of the commonest types. In this method, the servers refused to provide the services to genuine clients due to flooding of attacks or crashing of attacks.

43. Explain XSS attack and how to prevent it.

Cross-site scripting on XSS is a type of Cyber attack which leads to hackers injecting malicious client-side scripts into web pages. Xss is used for hijacking sessions or modifying the Dom or stealing cookies and remote code execution as well as crashing a given server.

44. What is an ARP and how does it work?

ARP or Address Resolution Protocol is a type of method for mapping an internet protocol address or the IP address with a physical machine address that is recognized within the Local Network. When the incoming packet for a host machine on a network is at the Gateway, it will ask the ARP program to find the actual MAC address of the device which matches its IP address.

45. What is port blocking within LAN?

Local Area Network (LAN) port blocking is defined as a method to restrict users from seeking out the service that is within the local area network and is called blocking. This type is used such that the destination nodes are not accessible and can be used only on the internet for one device running on it. These are used to prevent hacking of victims and stealing of data.

46. What protocols fall under the TCP/IP internet layer?

TCP/IP	Protocol Examples
Application	NFS, NIS+, DNS, rlogin, rsh, rcp, RIP, FTP and others
Transport	• TCP • UDP
Internet	• IP • ARP • ICM
Data Link	• PPP • IEEE 802.2
Physical Network	Ethernet (IEEE 802.3) Token ring or RS-232 and others

47. What is a Botnet?

When a number of related malicious program-carrying devices are connected to the internet they are called a botnet. . These related devices are controlled by a common attacking party to perform malicious activities e.g. send spam.

48. What are salted hashes?

Salted hashes are the use of random data for protecting passwords to receive a new password and creating a hash value for that password, where a random salt value and the combined value are also stored in the database. And this protects the system from dictionary attacks and is thus known as a hash attack.

49. Explain SSL and TLS.

SSL is defined as the method of secure socket layer for verifying the Identity of the center and nothing else. And SSL will help the person to ensure and track the person you are talking to but can also be tricked. TLS is a type of identification tool similar to SSL. But it ensures that there are improved security features and additional protection to the layer. These have to be used together.

50. What is data protection in transit vs data protection at rest?

When data is protected in transit the data goes only from the server to the client. The effectiveness of data protection is critical for ensuring that there is no loss of data.

Data protection at test- is when the database is on the hard drive. The data at rest is sometimes less vulnerable than the data in transit.

51. What is 2FA and how can it be implemented for public websites?

2FA or multiple-factor authentication is an extra layer of security. It uses the password and username but will also need special information only that should be known to the user such as the physical token itself. Authentication apps replace the need for verification code on text or call mail or email.

52. What is Cognitive Cybersecurity?

Cognitive cyber security is the application of artificial intelligence technologies for the human thought process to identify threats and protect physical and digital systems.

53. What is the difference between VPN and VLAN?

VPN the group workstations are within the same locations and in the same broadcast, the main logically segregated networks and have no physical connection. VLAN - this is related to remote access to the company network. The connection of two points within a secured and encrypted tunnel. There is no encryption technique involved and it slices the logical network into different sections to manage and secure different aspects.

54. Explain Phishing and how to prevent it.

Phishing is a common cyber attack where the cybercriminal acts like a trusted person and extricates sensitive and financial information from users or victims. Phishing attacks can be prevented by ensuring that firewalls are used, antivirus software and internet security are used and sensitive information is not included in web pages that cannot be trusted.

I hope You Love these Questions and If you Want to support Me then you can buy a coffee for me! Thanks,

https://www.buymeacoffee.com/surendrapander

My social medial accounts -

Twitter — https://twitter.com/technicalSure

YouTube —
https://www.youtube.com/channel/UCZq87M0I0-zEfLuyyfEeE6Q

Instagram —
https://www.instagram.com/surendra_choudhary1241/

Linkedin —
https://www.linkedin.com/in/surendra-pander-4066761b7/