Cyber Security Interview Questions

Click here to view the live version of the page

Top 75+ Cyber Security Interview Questions and Answers 2024

Cyber Security is one of the most highly sought-after careers in the IT industry now. The demand keeps growing as the need to get things online increases every day. It also poses the industry with the major concern of securing data assets to prevent misuse. The increase in cybercrimes has become a threat to major companies, which compels them to hire cybersecurity professionals like cybersecurity Engineers and Cyber security analysts. So, you can take advantage of this market trend and become a cyber security expert. Skim through these top 75 cyber security interview questions and answers to prepare yourself for the interview.

Cyber Security Basic Interview Questions

Intermediate Cyber Security Interview Questions

Advanced Cyber Security Interview Questions

Cyber Security Interview Questions for Freshers

Cyber Interview Questions for Experienced

Scenario-Based Cyber Questions and Answers

MCQs on Cyber Security

Cyber Security Salary Trends

Cyber Security Job Trends

Cyber Security Roles and Responsibilities

Conclusion

Did You Know?

- According to the National Library of Medicine, healthcare and banking industries were the easiest targets for cyber attacks, and email phishing threats were the most common source of data breaches during COVID-19.
- According to Economic Times the 2023 India Threat Landscape Report by Singapore-based cybersecurity firm Cyfirma, India is the most targeted country globally for cyber attacks.
- According to one of the articles on LinkedIn, quantum computers pose a significant threat to current encryption methods. The United States Department of Defense (DoD) DARPA is investing a lot in quantum research and development to have superiority in technology in times of threat.
- By 2025, the expected growth in cybersecurity-related jobs is around 20%, which exceeds the average job market growth.
- The biggest highlight In the field of cyber security, there are nearly zero unemployment rates.
- 95% of the data available in the world is not protected, which shows the importance of cyber security.
- On a daily basis, over 560,000 new malware programs are introduced into the market, with 1 billion malware programs already existing.

Cyber Security Basic Interview Questions

1. What is cryptography?

Cryptography refers to the domain of cyber security that serves the purpose of safeguarding information from individuals known as adversaries, thereby ensuring that the data is exclusively accessed by only senders and intended recipients.

2. What is a traceroute? Mention its uses.

Traceroute is a network diagnostic tool that helps track the route taken by a packet sent across the IP network. It also shows the IP addresses of all the routers it pinged between the source and the destination.

Uses:

- It shows the time taken by the packet for each hop during the transmission.
- When the packet is lost during the transmission, the traceroute will identify the point of failure.

3. What is a firewall? Mention its uses.

In cybersecurity, a firewall refers to a type of network security system that blocks malicious traffic from hackers and hence maintains the data privacy. This includes bots, phishing links, worms viruses, malware, trojan viruses, etc.

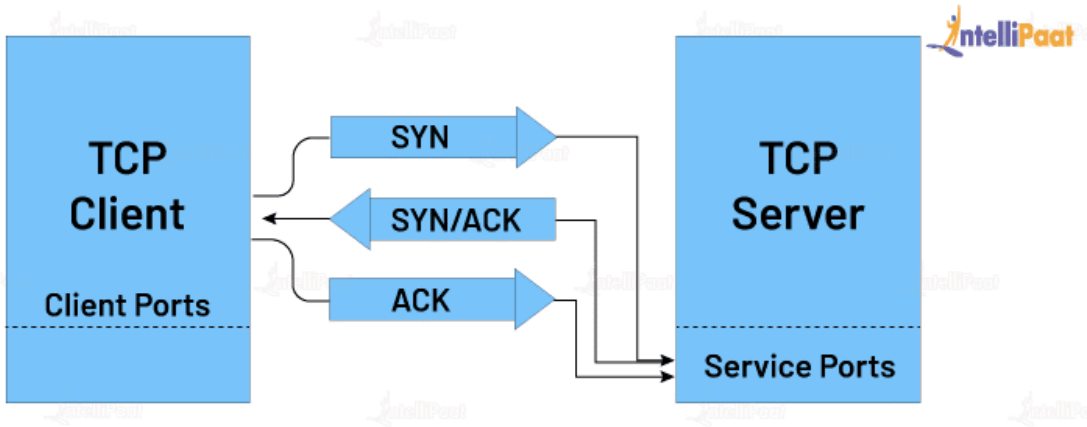
Uses:

- The firewall monitors the inbound and outbound network traffic. It permits or allows only data packets agreeable to the set of security guidelines the server owner sets.
- A firewall acts as a barrier between the internal network and the inbound traffic from external sources like the Internet.

Enroll in our Cyber Security course to learn from experts and get certified!

4. What is a three-way handshake?

It is a process that happens in a TCP/IP network when you make a connection between a local host and the server. It is a three-step process to negotiate the acknowledgment and synchronization of packets before communication starts.



Step 1: The client makes a connection with the server with SYN.

Step 2: The server responds to the client's request with SYN+ACK.

Step 3: The client acknowledges the server's response with ACK, and the actual data transmission begins.

5. What is a response code? List them.

HTTP response codes indicate a server's response when a client makes a request to the server. It shows whether an HTTP request is completed or not.

1xx: Informational

The request is received, and the process continues. Some example codes are:

- 100 (continue)
- 101 (switching protocol)
- 102 (processing)
- 103 (early hints)

2xx: Success

The action is received, understood, and accepted successfully. A few example codes for this are:

- 200 (OK)
- 202 (accepted)
- 205 (reset content)
- 208 (already reported)

3xx: Redirection

To complete the request, further action is required to take place. Example codes:

- 300 (multiple choice)
- 302 (found)
- 308 (permanent redirect)

4xx: Client Error

The request has incorrect syntax, or it is not fulfilled. Here are the example codes for this:

- 400 (bad request)
- 403 (forbidden)
- 404 (not found)

5xx: Server Error

The server fails to complete a valid request. Example codes for this are:

- 500 (internal server error)
- 502 (bad gateway)
- 511 (network authentication required)

Also, check out this blog for Top Cyber Security Skills!

6. What is the CIA triad?

CIA Triad is a security model to ensure IT security. CIA stands for confidentiality, integrity, and availability.

- Confidentiality: To protect sensitive information from unauthorized access.
- Integrity: To protect data from deletion or modification by an unintended person.
- Availability: To confirm the availability of the data whenever needed.

7. Name various types of cyberattacks.

Here is a list of common cyberattacks aimed at inflicting damage to a system.

1. Man in the Middle attack: The attacker puts himself in the communication between the sender and the receiver. This is done to eavesdrop and impersonate to steal data.
2. Phishing: Here, the attacker will act as a trusted entity to perform malicious activities such as getting usernames, passwords, and credit card numbers.
3. Rogue Software: It is a fraudulent attack where the attacker fakes a virus on the target device and offers an anti-virus tool to remove the malware. This is done to install malicious software into the system.
4. Malware: Malware is software that is designed to attack the target system. The software can be a virus, worm, ransomware, spyware, and so on.
5. Drive-by Downloads: The hacker takes advantage of the lack of updates on the OS, app, or browser, which automatically downloads malicious code to the system.
6. DDoS: This is done to overwhelm the target network with massive traffic, making it impossible for the website or the service to be operable.
7. Malvertising: Malvertising refers to the injections of maleficent code to legitimate advertising networks, which redirect users to unintended websites.
8. Password Attacks: As the name suggests, here, the hacker obtain credentials like passwords.

Check out our blog on Cyber Security Tips and Best Practices to prevent Cyber Security attacks!

8. What is data leakage?

Data leakage is the term used to describe the unauthorized release of data from a business to a third party. The internet, email, mobile data, as well as storage devices like USB keys, laptops, and optical discs, are just a few of the routes via which this transmission may take place.

Types of data leakage:

- Accidental leakage: The authorized entity sends data to an unauthorized entity accidentally.
- Malicious insiders: The authorized entity intentionally sends data to an unauthorized entity.
- Electronic communication: Hackers make use of hacking tools to intrude the system.

9. Explain port scanning.

A port scan helps you determine the ports that are open, listening, or closed on a network. Administrators use this to test network security and the system's firewall strength. For hackers, it is a popular reconnaissance tool to identify the weak point to break into a system.

Some of the common basic port scanning techniques are:

1. UDP
2. Ping scan
3. TCP connect
4. TCP half-open
5. Stealth scanning

Check out this interesting blog on Ethical Hacking Tools now!

10. Explain brute force attacks and the ways to prevent them.

A brute force attack is a hack where the attacker tries to guess the target password by trial and error. It is mostly implemented with the help of automated software used to login with credentials.

Here are some ways to prevent a brute force attack:

1. Set a lengthy password
2. Set a high-complexity password
3. Set a limit for login failures

Intermediate Cyber Security Interview Questions

11. What is cryptography?

Cryptography is a domain of cyber security, and its main purpose is to keep information safe from individuals known as adversaries and ensure data is accessed by only senders and intended recipients.

12. What is a firewall? Mention its uses.

A firewall in cybersecurity is like a wall that keeps track of incoming and outgoing traffic to block any malicious activity from hackers. This acts like a network security system that can maintain data privacy. Some malicious activities include bots, phishing links, worms viruses, malware, trojan viruses, etc.

Uses:

- Firewall checks if there are any data violations by monitoring the inbound and outbound network traffic. Data packets with an agreeable set of security guidelines set by the server owner are permitted.
- It is like a wall, keeping the internal network and outer traffic separate from external sources like the internet.

13. What is the CIA triad?

The CIA in CIA Triad stands for confidentiality, integrity, and availability, which is one of the most common models used to ensure IT security. Let's see what confidentiality, integrity, and availability mean:

- Confidentiality: This is mainly to protect private information from unauthorized access.
- Integrity: This is all about the protection of data from being deleted or modified by unauthorized people.
- Availability: This is to check if data is available when it's required.

14. Name various types of cyberattacks.

Below is a list of cybersecurity attacks that aim to cause damage to the system.

- Man in the Middle Attack: As the name suggests, an attacker puts himself in the middle of the communication between the sender and receiver to steal data by eavesdropping.
- Phishing: This type of attack is when the attacker acts like someone trustworthy by sending links from reputed sources and then stealing your information, like usernames, passwords, and credit card numbers.
- Rogue Software: This type of attack is when the attacker fakes by making the target believe they have a virus in their system and offers an anti-virus tool to remove the virus. This is done to install the malware software on the target's system.

- Malware: This is software that is intentionally created to cause harm to the target's system. The type of software can be a virus, worm, ransomware, spyware, and so on.
- Drive-by Downloads: This is a type of attack that occurs when the target unknowingly installs a virus. The hacker takes advantage of the lack of updates on OS, apps, or browsers, which can automatically install virus code into the system.
- DDoS: A Distributed Denial of Service attack is when the target's network, for example, gets a huge amount of traffic at a time, forcing the website to reach its limit and not operate.
- Malvertising: This is a type of attack where a harmful malware code is injected into a legitimate advertisement, which will redirect a user to an unintended website.
- Password Attacks: As the name suggests, the hacker takes advantage of the tendency of users to give easy passwords by researching their online-given information. This can then be used to access password-protected information.

15. What is a response code? List them.

An HTTP response code is a response that the server gives to a client's request. It is indicated if an HTTP request is completed or not. Below are the code statuses and their categories:

1xx: Informational

This tells us that the request has been received and the process can continue. Below are some of the sample code statuses:

- 100 (continue)
- 101 (switching protocol)
- 102 (processing)
- 103 (early hints)

2xx: Success

This code indicates that the action was successful by receiving, understanding, and accepting the information.

- 200 (OK)
- 202 (accepted)
- 205 (reset content)
- 208 (already reported)

3xx: Redirection

This code status indicates that to complete the request, an additional action is required. Below are some examples of the codes:

- 300 (multiple choice)
- 302 (found)
- 308 (permanent redirect)

4xx: Client Error

This indicates that the requested page couldn't be reached or the request has a syntax error. Below are some of the code examples:

- 400 (bad request)
- 403 (forbidden)
- 404 (not found)

5xx: Server Error

This status is when the server is not able to complete the valid request. Below are some code examples:

- 500 (internal server error)
- 502 (bad gateway)
- 511 (network authentication required)

16. What is a traceroute? Mention its uses.

Traceroute is a network analytical tool that helps track the way taken by a packet traveling across the IP (Internet Protocol) network. It also shows the IP addresses of all the routers moving from the source to the destination.

Uses:

- It shows the time taken by the packet for each hop during the transmission, where hop is the move our data makes to go from one point to another.
- When the packet is lost during the transmission, the traceroute will identify the point of failure. This is done by receiving an ICMP time exceeded message from the hop, which tells us that the time-to-live value of that packet has reached zero.

17. What is a three-way handshake?

A three-way handshake is a term given to the process of making the connection between a local host and the server in a TCP/IP network. As the name suggests, it is a three-way process where a reliable connection is set up between 2 devices with synchronization (SYN) and acknowledgment (ACK) before sharing of data.

Step 1: The client first sends a synchronization (SYN) to the server to make the connection.
Step 2: The server then responds to the client's request with synchronization (SYN) and acknowledgment (ACK).
Step 3: The client sends back an acknowledgment (ACK) to the server's response, telling that the connection was established.

18. What is data leakage?

Data leakage is when unauthorized information about a business is sent to a third party via the internet, mobile data, email, USK keys, laptops, etc.

Types of data leakage:

- Accidental leakage: As the name suggests, this is when an authorized person accidentally sends the information to an unauthorized person.
- Malicious insiders: This is when an authorized person sends data to an unauthorized person intentionally.
- Electronic communication: This is when a hacker uses different hacking tools to enter the system.

19. Explain brute force attacks and the ways to prevent them.

This is an attack where the attacker tries to guess the password with trial and error. This is done with the help of software used to log in with credentials.

Here are some ways to prevent a brute force attack:

1. Set a lengthy password
2. Set a high-complexity password
3. Set a limit for login failures

20. Explain port scanning.

A port scan helps to check for open ports, listening, or closed on a network. This is used by administrators to check for network security and the system's firewall strength. This is a popular exploration tool to identify the weak point in the system to break in.

Some of the common basic port scanning techniques are:

1. UDP
2. Ping scan
3. TCP connect
4. TCP half-open
5. Stealth scanning

21. Distinguish between HIDS and NIDS.

Host Intrusion Detection System	Network Intrusion Detection System
Detects the attacks that involve hosts	Detects attacks that involve networks
Analyzes what a particular host/application is doing	Examines the network traffic of all devices
Discovers hackers only after the machine is breached	Discovers hackers at the time they generate unauthorized attacks

22. Mention the difference between symmetric and asymmetric encryption.

Differentiator	Symmetric Encryption	Asymmetric Encryption
Encryption Key	Only one key to encrypt and decrypt a message	Two different keys (public and private keys) to encrypt and decrypt the message
Speed of Execution	Encryption is faster and simple	Encryption is slower and complicated
Algorithms	RC4, AES, DES, and 3DES	RSA, Diffie-Hellman, and ECC

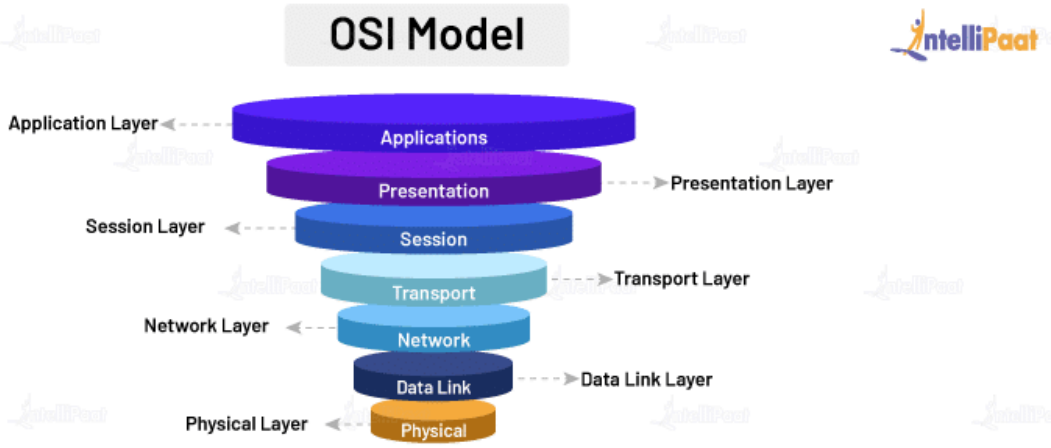
Usage	For the transmission of large chunks of data	For smaller transmission to establish a secure connection prior to the actual data transfer

23. What is the difference between IDS and IPS?

Intrusion Detection System	Intrusion Prevention System
A network infrastructure to detect intrusion by hackers	A network infrastructure to prevent intrusions by hackers
Flags invasion as threads	Denies the malicious traffic from threads
Detects port scanners, malware, and other violations	Does not deliver malicious packets if the traffic is from known threats in databases

24. What are the different layers of the OSI model?

The OSI model was introduced by the International Organization for Standardization for different computer systems to communicate with each other using standard protocols.



Below are the various layers of the OSI model:

- Physical layer: This layer allows the transmission of raw data bits over a physical medium.
- Data Link layer: This layer determines the format of the data in the network.
- Network layer: It tells which path the data will take.
- Transport layer: This layer allows the transmission of data using TCP/UDP protocols.
- Session layer: It controls sessions and ports to maintain the connections in the network.
- Presentation layer: Data encryptions happen in this layer, and it ensures that the data is in a usable/presentable format.
- Application layer: This is where the user interacts with the application.

25. What is a VPN?

Your online activities are protected from the risks of a public internet connection by a virtual private network, or VPN, which establishes a private and secure network. You may protect tasks like sending emails, making online payments, and conducting e-commerce by utilizing a VPN to increase your anonymity and privacy.

Working of VPN

1. When you make a VPN connection, your device routes the internet connection to the VPN's private server, instead of your Internet Service Provider (ISP).
2. During this transmission, your data is encrypted and sent through another point on the internet.
3. When it reaches the server, the data is decrypted.
4. The response from the server reaches the VPN where it is encrypted, and it will be decrypted by another point in the VPN.
5. At last, the data, which is decrypted, reaches you.

Are you excited to know about the Access Control List, so check out this blog!

26. What do you understand by risk, vulnerability, and threat in a network?

- A cyber security threat possesses the potential to harm an organization's assets by exploiting vulnerabilities, whether intentional or accidental.
- A vulnerability represents a security system weakness or gap that can be exploited by malicious hackers.
- Risk emerges when a threat successfully exploits a vulnerability, leading to loss, destruction, or damage to assets.

27. How do you prevent identity theft?

To prevent identity theft, you can take the following measures:

1. Protect your personal records.

2. Avoid online sharing of confidential information.
3. Protect your AADHAR/Social Security Number.
4. Use strong passwords, and change them at regular intervals.
5. Do not provide your bank information on untrustworthy websites.
6. Protect your system with advanced firewall and spyware tools.
7. Keep your browsers, system, and software updated.

Enroll in our Cyber Security Course in Bangalore to upskill yourself!

28. Who are White Hat, Grey Hat, and Black Hat Hackers?

Black Hat Hackers

A black hat hacker uses his/her hacking skills to breach confidential data without permission. With the obtained data, the individual performs malicious activities such as injecting malware, viruses, and worms.

White Hat Hackers
A white hat hacker uses his/her hacking skills to break into a system but with the permission of the respective organizations. They are professionals known as Ethical Hackers. They hack the system to identify its vulnerability and to fix it before a hacker takes advantage of it.

Grey Hat Hackers

A grey hat hacker has the characteristics of both a black hat hacker and a white hat hacker. Here, the system is violated with no bad intention but they do not have the essential permission to surf the system, so it might become a potential threat at any time.

Check out this interesting blog on Cyber Security Consultant Career!

29. When should you do patch management, and how often?

Immediate action is required to perform patch management as soon as software updates are released. It is crucial that all network devices within the organization undergo patch management within a timeframe of one month or less.

30. What are the ways to reset a password-protected BIOS configuration?

BIOS being hardware, setting it up with a password locks the operating system. There are three ways to reset the BIOS password:

1. you need to unplug the PC and remove the CMOS battery in the cabinet for 15–30 minutes. Then, you can put it back.
2. You can use third-party software such as CmosPwd and Kiosk.
3. You can run the below commands from the MS-DOS prompt with the help of the debug tool. For this method to work, you need to have access to the OS installed.

```
Debug

o 70 2E

o 71 FF

quit
```

This will reset all BIOS configurations, and you will need to re-enter the settings for it.

31. Explain the MITM attack. How to prevent it?

In the Man-in-the-Middle attack, the hacker eavesdrops on the communication between two parties. The individual then impersonates another person and makes

the data transmission look normal for the other parties. The intent is to alter the data, steal personal information, or get login credentials for sabotaging communication.

These are a few ways to prevent a MITM attack:

1. Public key pair based authentication
2. Virtual private network
3. Strong router login credentials
4. Implement a well-built Intrusion Detection Systems (IDS) like firewalls.
5. Strong WEP/WPA encryption on access points

32. Explain the DDoS attack. How to prevent it?

Distributed denial-of-service attack overwhelms the target website, system, or network with huge traffic, more than the server's capacity. The aim is to make the server/website inaccessible to its intended users. A DDoS attack happens in the below two ways:

Flooding attacks: This is the most commonly occurring type of DDoS attack. Flooding attacks stop the system when the server is accumulated with massive amounts of traffic that it cannot handle. The attacker sends packets continuously with the help of automated software.

Crash attacks: This is the least common DDoS attack where the attacker exploits a bug in the targeted system to cause a system crash. It prevents legitimate users from accessing email, websites, banking accounts, and gaming sites.

To prevent a DDoS attack, you have to:

1. Configure firewalls and routers
2. Recognize the spike in traffic
3. Consider front-end hardware
4. Empower the server with scalability and load balancing
5. Use anti-DDoS software

Also, Read on: Intrusion Prevention System to enhance your Knowledge!

33. Explain the XSS attack. How to prevent it?

Cross-site scripting also known as XSS attack allows the attacker to pretend as a victimised user to carry out the actions that the user can perform, in turn, stealing any of the user's data. If the attacker can masquerade as a privileged victimised user, one can gain full control over all the application's data and functionality. Here, the attacker injects malicious client-side code into web services to steal information, run destructive code, take control of a user's session, and perform a phishing scam.

Here are the ways to prevent an XSS attack:

1. Cross-check the user's input
2. Sanitize HTML
3. Employ anti-XSS tools
4. Use encoding
5. Check for regular updates of the software

34. What is an ARP, and how does it work?

Address Resolution Protocol is a communication protocol of the network layer in the OSI model. Its function is to find the MAC address for the given IP address of the system. It converts the IPv4 address, which is 32-bit, into a 48-bit MAC address.

How ARP works:

1. It sends an ARP request that broadcasts frames to the entire network.

2. All nodes on the network receive the ARP request.
3. The nodes check whether the request matches with the ARP table to find the target's MAC address.
4. If it does not match, then the nodes silently discard the packet.
5. If it matches, the target will send an ARP response back to the original sender via unicast.

35. What is port blocking within LAN?

Port blocking within LAN involves the act of preventing users from accessing a specific set of services within the local area network. The primary objective is to halt the source's capability to grant access to destination nodes through ports. As all applications operate on ports, it becomes crucial to obstruct these ports in order to limit unauthorized access, which could potentially exploit security vulnerabilities within the network infrastructure.

Advanced Cyber Security Interview Questions and Answers

36. What are the protocols that fall under the TCP/IP Internet layer?

Application Layer	NFS, NIS, SNMP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, DNS, LDAP, and others
Transport Layer	TCP, SCTP, UDP, etc.
Internet	IPv4, ARP, ICMP, IPv6, etc.

Data Link Layer	IEEE 802.2, PPP, etc.
Physical Layer	Ethernet (IEEE 802.3), FDDI, Token Ring, RS-232, and others

37. What is a botnet?

A botnet, also called a robot network, is a malware that infects networks of computers and gets them under the control of a single attacker who is called a 'bot herder.' A bot is an individual machine that is under the control of bot herders. The attacker acts as a central party who can command every bot to perform simultaneous and coordinated criminal actions.

A botnet is usually always responsible for large-scale attacks since a bot herder can control millions of bots at a time. All the bot can receive updates from the attacker to change their behavior in no time.

38. What is a CSRF attack? How is it executed?

Cross-Site Request Forgery (CSRF) attack, also known as session riding or one-click attack, is a malicious exploit that tricks a victim into performing unintended actions on a website on which they are authenticated. It occurs when an attacker exploits the trust between a user's browser and a targeted website. The attack takes advantage of the fact that websites often rely on cookies or other authentication credentials to verify a user's identity.

In order to execute a CSRF attack, an attacker typically follows these steps:

1. Identify the Target: The attacker selects a target website or web application that has a vulnerability that can be exploited through CSRF.
2. Craft the Malicious Payload: The attacker creates a malicious payload, typically in the form of HTML or JavaScript code, which will be executed by the victim's browser.

3. Create a Malicious Website: The attacker sets up a malicious website or incorporates the malicious payload into a legitimate website that they control. This website will be used to trick the victim into unknowingly performing actions on the target website.
4. Exploit the Trust Relationship: The attacker entices the victim to visit the malicious website. This can be done through social engineering techniques such as sending phishing emails, distributing malicious advertisements, or leveraging cross-site scripting (XSS) vulnerabilities.
5. Victim Interaction: When the victim visits the malicious website, the malicious payload is executed in their browser without their knowledge. The payload contains requests designed to mimic legitimate actions on the target website.
6. Sending Forged Requests: The victim's browser automatically sends HTTP requests to the target website, carrying out actions on behalf of the victim. These requests can include changing account settings, making purchases, or performing any action that the victim's account is authorized to do.
7. Exploiting Authentication: The target website receives the forged requests and processes them, assuming they are legitimate due to the victim's authenticated session (e.g., session cookies) with the website. As a result, the actions requested by the attacker are performed on the victim's behalf.
8. Attack Success: If the CSRF attack is successful, the attacker achieves their desired outcome, which can range from unauthorized actions to data theft, depending on the vulnerability and the attacker's intentions.

39. What are salted hashes?

When two users have the same password, it will result in the creation of the same password hashes. In such a case, an attacker can easily crack the password by performing a dictionary or brute-force attack. To avoid this, a salted hash is implemented.

A salted hash is used to randomize hashes by prepending or appending a random string (salt) to the password before hashing. This results in the creation of two completely different hashes, which can be employed to protect the users' passwords in the database against the attacker.

40. What is ARP poisoning?

Address Resolution Protocol (ARP) poisoning, also known as ARP spoofing or ARP cache poisoning, is a type of cyber attack where an attacker manipulates the ARP tables on a local area network (LAN). The attack involves sending falsified ARP messages to associate the attacker's MAC address with the IP address of another device on the network, redirecting network traffic intended for that device to the attacker.

41. Explain SSL and TLS.

Secure Sockets Layer (SSL)

It employs encryption algorithms to keep any sensitive data that is sent between a client and a server by scrambling the data in transit. This helps prevent hackers from reading any data, such as credit card details and personal and other financial information; it is done by keeping the internet connection secure.

Transport Layer Security (TLS)

TLS is the successor of SSL. It is an improved protocol version that works just like SSL to protect information transfer. However, to provide better security, both TLS and SSL are often implemented together.

Stay one step ahead: Enhance your knowledge of application security and proactively mitigate risks in your software!

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

Data Protection in Transit	Data Protection at Rest
Data is transmitted across devices or networks	Data is stored in databases, local hard drives, or USBs
Protects the data in transit with SSL and TLS	Protects the data at rest with firewalls, antiviruses, and good security practices
You must protect the data in transit since it can become vulnerable to MITM attacks, eavesdropping, etc.	You should protect the data at rest to avoid possible data breaches even when stolen or downloaded

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

Two-factor authentication (2FA) requires a password, along with a unique form of identification like a login code via text message (SMS) or a mobile application, to verify a user. When the user enters the password, they are prompted to enter the security code to log in to the website. If the code mismatches, the user will be blocked from entering the website.

Examples of 2FA: Google Authenticator, YubiKey, Microsoft Authenticator, etc.

Let's get a dive into the Cyber Security Interview Questions for Freshers.

Cyber Security Interview Questions for Freshers

44. Differentiate between hashing and encryption.

Hashing	Encryption
A one-way function where you cannot decrypt the original message	Encrypted data can be decrypted to the original text with a proper key
Used to verify data	Used to transmit data securely
Used to send files, passwords, etc. and to search	Used to transfer sensitive business information

Looking for a rewarding career in ethical hacking? Enroll in our Ethical Hacking course and pave the way for success!

45. What is the difference between vulnerability assessment (VA) and penetration testing (PT)?

Vulnerability Assessment (VA)	Penetration Testing (PT)
Identifies the vulnerabilities in a network	Identifies vulnerabilities to exploit them to penetrate the system
Tells how susceptible the network is	Tells whether the detected vulnerability is genuine
Conducted at regular intervals when there is a change in the system or network	Conducted annually when there are significant changes introduced into the system

46. What is SSL encryption?

The Secure Socket Layer (SSL) functions as a security protocol utilized for encryption, enabling network privacy, data integrity, and authentication, particularly in scenarios like online transactions.

1. To establish SSL encryption, the following steps are undertaken in an active tone:
2. The browser initiates a connection with an SSL-secured web server.
3. The browser requests the server's public key while providing its own private key.
4. Upon confirming the server's trustworthiness, the browser proceeds to establish an encrypted connection with the web server.
5. The web server acknowledges the request and commences an SSL-encrypted connection.
6. SSL communication takes place between the browser and the web server.

47. Define a zero-day vulnerability.

A zero-day vulnerability refers to a security flaw or weakness in a software application or system that is unknown to the vendor or developers, leaving it exposed to potential exploitation by attackers. The term “zero-day” implies that the vulnerability is discovered and exploited by hackers before the software vendor becomes aware of it, giving them zero days to address and patch the vulnerability. As a result, no official fixes or countermeasures are available to protect against such attacks.

Some examples of zero-day vulnerabilities are the following:

- Stuxnet Worm in 2010
- Petya Ransomware in 2016
- Adobe Flash Player in 2015

48. With the differential parameters, differentiate between HTTP and HTTPS.

Below mentioned are the differences between HTTP and HTTPS protocols:

Parameters	HTTP (Hypertext Transfer Protocol)	HTTPS (Hypertext Transfer Protocol Secure)
Protocol Type	Unsecured	Secured
Encryption	No encryption	SSL/TLS encryption
Port	Port 80	Port 443
Data Security	Data is sent in plain text.	Data is encrypted before transmission.
Authentication	No built-in authentication mechanism	Utilizes SSL/TLS certificates for authentication
URL Scheme	Begins with “http://”	Begins with “https://”
Security Risk	Prone to eavesdropping and data interception	Protects against eavesdropping and data interception

49. What countermeasures will you take to secure a server?

A server that is secured uses the Secure Socket Layer (SSL) protocol to encrypt and decrypt data to protect it from unauthorized access.

Below are the four steps to secure a server:

Step 1: Secure the root and administrator users with a password

Step 2: Create new users who will manage the system

Step 3: Do not give remote access to administrator/default root accounts

Step 4: Configure firewall rules for remote access

Cyber Interview Questions for Experienced

50. What do you mean by Cognitive Cybersecurity?

Cognitive Cybersecurity is a way of using human-like thought mechanisms and converting them to be used by Artificial Intelligence technologies in cyber security to detect security threats. It is to impart human knowledge to the cognitive system, which will be able to serve as a self-learning system. This helps identify the threats, determine their impact, and manifest reactive strategies.

51. What is the difference between VPN and VLAN?

Virtual Private Network	Virtual Local Area Network

Provides secure remote access to a company's network resources	Used to group multiple computers that are geographically in different domains into the same geographical broadcast domain
A network service	A way of subnetting the network
Companies wishing to connect with their remote employees will use a VPN	Companies wishing to employ traffic control and easier management will use a VLAN

52. Explain phishing and how you prevent it.

In phishing, an attacker masquerades as a trusted entity (a legitimate person/company) to obtain sensitive information by manipulating the victim. It is achieved by any kind of user interaction, such as asking the victim to click on a malicious link and to download a risky attachment, to get confidential information such as credit card information, usernames, passwords, and network credentials.

The following are some of the ways to prevent phishing:

1. Install firewalls
2. Rotate passwords frequently
3. Do not click on or download from unknown sources
4. Get free anti-phishing tools
5. Do not provide your personal information on an unsecured/unknown site

53. Explain SQL injection. How can we prevent it?

SQL injection is an injection attack where an attacker executes malicious SQL commands on the database server, including MySQL, SQL Server, or Oracle, that runs behind a web application. The intent is to gain unauthorized access to

sensitive data such as client information, personal information, intellectual property details, and so on. In this attack, the attacker can add, modify, and delete records in the database, which results in the loss of data integrity in an organization.

Ways to prevent SQL injection:

1. Limit providing read access to the database
2. Sanitize data with the limitation of special characters
3. Validate user inputs
4. Use prepared statements
5. Check for active updates and patches

54. Mention the steps used for configuring a firewall.

The steps mentioned below need to be followed to set up a password:

1. Username/password: Alter the default password of a firewall device.
2. Remote Administration: Always disable the Remote Administration feature.
3. Port Forward: For the web server, FTP, and other applications to work properly, configure appropriate ports.
4. DHCP Server: Disable the DHCP server when you install a firewall to avoid conflicts.
5. Logging: Enable logs to view the firewall troubleshoots and to view logs.
6. Policies: Configure strong security policies with the firewall.

Want to know How to become a cyber security engineer in 2023? check this blog out!

55. Explain phishing and how do you prevent it?

In phishing, an attacker masquerades as a trusted entity (as a legitimate person/company) to obtain sensitive information by manipulating the victim. It is achieved by any kind of user interaction, such as asking the victim to click on a malicious link and to download a risky attachment, to get confidential information such as credit card information, usernames, passwords, and network credentials.

The following are some of the ways to prevent phishing:

1. Install firewalls
2. Rotate passwords frequently
3. Do not click on or download from unknown sources
4. Get free anti-phishing tools
5. Do not provide your personal information on an unsecured/unknown site

56. Explain SQL injection. How to prevent it?

SQL injection is an injection attack where an attacker executes malicious SQL commands in the database server, including MySQL, SQL Server, or Oracle, that runs behind a web application. The intent is to gain unauthorized access to sensitive data such as client information, personal information, intellectual property details, and so on. In this attack, the attacker can add, modify, and delete records in the database, which results in the loss of data integrity in an organization.

Ways to prevent SQL injection:

1. Limit providing read access to the database
2. Sanitize data with the limitation of special characters
3. Validate user inputs
4. Use prepared statements
5. Check for active updates and patches

Have a look at this Cyber Security Tutorial, which will make it easier for you to dive into this field!

Scenario-based Cyber Security Interview Questions and Answers

57. You have a suture from where you receive the following email from the help desk:

Dear YYY,

We are deleting all inactive emails to create space for other new users. If you want to save your account data, please provide the following details: First Name and Last Name:
Email ID:
Password:
Date of Birth:
Alternate Email: Please submit the above detail by the end of the week to avoid any account termination.

The above email is an excellent illustration of phishing. Here are the reasons why:

1. A reputed organization will never ask for an employee's personal information in the mail.
2. In a normal mail, the salutation is not done in a generalized manner. This happens only in spam emails where the attacker tricks you into 'biting.'

As a rule of thumb, you should never revert to a sender who demands personal information and passwords via emails, phone calls, text messages, and instant messages (IMs). You must not disclose your data to any external party even if the sender works for organizations such as ITS or UCSC.

58. You get an e-card in your mail from a friend. It asks you to download an attachment to view the card. What will you do? Justify your answer.

1. Do not download the attachment as it may have viruses, malware, or bugs, which might corrupt your system.
2. Do not visit any links as they might redirect you to an unintended page.

3. As fake email addresses are common and easy to create, you should not perform any action like clicking/downloading any links, unless you confirm it with the actual person.
4. Many websites masquerade as legitimate sites to steal sensitive information, so you should be careful not to fall into the wrong hands.

59. A staff member in a company subscribes to various free magazines. To activate the subscription, the first magazine asks her for her birth month, the second magazine asks for her birth year, and the third magazine asks for her maiden name. What do you deduce from the above situation? Justify your answer.

It is highly likely that the above-mentioned three newsletters are from a parent company, which are distributed through different channels. It can be used to gather essential pieces of information that might look safe in the user's eyes. However, this can be misused to sell personal information to carry out identity theft. It might further ask the user for the date of birth for the activation of the fourth newsletter.

In many scenarios, questions that involve personal details are unnecessary, and you should not provide them to any random person, company, or website unless it is for a legitimate purpose.

60. Case study:In our computing labs and departments, the print billing system is typically linked to the user's login. Users log in, initiate print jobs, and subsequently receive a bill for the printed material, either individually or through their respective departments. Occasionally, individuals contact us to express their dissatisfaction

with invoices for printing they claim they did not perform, only to discover that the bills are, in fact, accurate. Question: What do you believe could be the underlying issue in this situation?

To avoid this situation, you should always sign out of all accounts, close the browser, and quit the programs when you use a shared or public computer. There are chances that an illegitimate user can retrieve your authorized data and perform actions on behalf of you without your knowledge when you keep the accounts in a logged-in state.

61. What is DMZ in cybersecurity?

DMZ stands for demilitarized zone. It is a network architecture that acts as a buffer zone between an organization's internal network and an external or untrusted network, typically the internet. The purpose of a DMZ is to provide an additional layer of security by segregating and isolating certain systems or services that need to be accessible from the internet.

The DMZ is designed to host publicly accessible services such as web servers, email servers, or FTP servers that need to be accessed by users outside the organization. Placing these services in the DMZ separates them from the internal network, reducing the potential attack surface and minimizing the risk to sensitive resources and data. A DMZ is implemented using firewalls and network segmentation techniques.

Typically, two firewalls are employed: one facing the internet and another separating the DMZ from the internal network. The external-facing firewall allows limited and controlled inbound traffic to reach the DMZ, while the internal-facing firewall enforces strict rules to prevent unauthorized access from the DMZ to the internal network.

62. Differentiate between DDoS and DoS attack.

Parameters	DDoS Attack	DoS Attack
Attack Method	DDoS attacks involve multiple sources, often compromised computers or devices forming a botnet. These sources collectively bombard the target with a massive volume of traffic or requests, making it difficult to mitigate the attack.	A single source or a small group of sources flood the target system or network with a high volume of traffic or requests, overwhelming its resources and causing service disruption or denial.
Source of Attack	DDoS attacks utilize a distributed network of compromised devices, making it harder to identify and mitigate the attack. The sources are often geographically dispersed.	A DoS attack typically originates from a single source or a limited number of sources under the attacker's control.
Scale and Impact	DDoS attacks can generate an enormous volume of traffic, overwhelming even robust systems or networks. They have a larger scale and can lead to	Due to the limited resources of a single source or a few sources, a DoS attack generally has a smaller scale and impact. It may cause a

	significant downtime, rendering services completely inaccessible.	temporary disruption or slowdown of services.
Complexity and Coordination	DDoS attacks demand more resources, planning, and coordination to compromise multiple devices and coordinate the attack. They involve exploiting vulnerabilities and establishing control over a network of compromised machines.	Implementing a DoS attack requires less coordination and resources. It can be launched by an individual or a small group using readily available tools or scripts.
Detection and Mitigation	DDoS attacks are more challenging to detect and mitigate due to the distributed nature of the attack traffic. Advanced DDoS mitigation solutions are required, involving traffic analysis, rate limiting, or employing cloud-based DDoS protection services.	Detecting and mitigating DoS attacks is relatively straightforward since the attack traffic often originates from a single or a few sources. Filtering or blocking the source IP addresses can help mitigate the attack.
Motivation	DDoS attacks can have similar motivations as DoS attacks, but they are more frequently associated with organized crime, hacktivism, or state-sponsored actors attempting to cause widespread disruption or target specific organizations or infrastructure.	DoS attacks are often carried out by individuals or groups seeking to disrupt services, gain a competitive advantage, or settle personal grudges.

63. Case study: In your college computer lab, one of your friends logged into her email account. When she left the lab, she only logged out from her email account. Later, she received a notification that someone had re-accessed her account from the college computer system's browser, which she has used to send emails. Question- How do you think this happened?

There are two possible scenarios:

1. The attacker can visit the browser's history to access her account if she hasn't logged out.
2. Even if she has logged out but has not cleared the web cache (pages a browser saves to gain easy and quick access for the future)

64. Case study: An employee's bank account faces an error during a direct deposit procedure. Two different offices need to work on it to straighten this out. Office #1 contacts Office #2 by email to send the valid account information for the deposit. The employee now gives the bank confirmation that the error no longer exists. Question- What is wrong here?

Any sensitive information cannot be shared via email as it can lead to identity theft. This is because emails are mostly not private and secure. Sharing or sending personal information along the network is not recommended as the route can be easily tracked.

In such scenarios, the involved parties should call each other and work with ITS as a secure way of sending the information.

Check out this interesting blog on the difference between Cyber Security and Information Security!

65. You see an unusual activity of the mouse pointer, which starts to move around on its own and clicks on various things on the desktop. What should you do in this situation?

A. Call any of the co-workers to seek help
B. Disconnect the mouse
C. Turn your computer off
D. Inform the supervisor
E. Disconnect your computer from the network
F. Run anti-virus
G. Select all the options that apply?

Which options would you choose?

The answer is (D) and (E). This kind of activity is surely suspicious as an unknown authority seems to have the access to control the computer remotely. In such cases, you should immediately report it to the respective supervisor. You can keep the computer disconnected from the network till help arrives.

66. Check out the list of passwords below, which are pulled out from a database and choose the passwords that are in line with the UCSC's password requirements:

A. Password1
B. @#$)*&^%
C. UcSc4Evr!
D. akHGksmLN

Choose the passwords that are in line with the UCSC's password requirements.

The answer is C (UcSc4Evr!). As per the UCSC requirements, a password should be:

1. Minimum of 8 characters in length
2. Having any of the three from these four types of characters: lower case, upper case, numbers, and special characters.

67. The bank sends you an email, which says it has encountered a problem with your account. The email is provided with instructions and also a link to log in to the account so that you can fix it. What do you infer from the above situation? Explain.

It appears to be an unsolicited email. You should report it as spam and move the email to the trash immediately in the respective web client you use (Yahoo Mail, Gmail, etc.). Before providing any bank-related credentials online, you should call the bank to check if the message is legitimate and is from the bank.

68. In your IT company, employees are registering numerous complaints that the campus computers are delivering Viagra spam. To verify it, you check the reports, and it turns out to be correct. The computer program is automatically sending tons of spam emails without the owner's knowledge. This happened because a hacker had installed a malicious program into the system. What are the reasons you think might have caused this incident?

This type of attack happens when the password is hacked. To avoid this, whenever you set a password, always use a proper standard, i.e., use passwords that are at least 8-character length and have a combination of upper case/lower case letters, symbols/special characters, and numbers.

Other scenarios of the above attack could be:

1. Dated antivirus software or the lack of it
2. Dated updates or security patches

That's all for now!

This blog has listed answers to the most frequently asked Cyber Security analyst interview questions. The answers provided here aim to help you have an understanding of Cyber Security basics. You have also understood how you can implement the concepts practically in the real world through scenario-based questions. Hope this will help you crack your next Cybersecurity interview.

Cyber Security Salary Trends

69. You've been notified of a potential ransomware attack on your network. What are your immediate steps to contain the damage and mitigate the attack?

Here are some immediate steps to contain the damage and mitigate the attack:

1. Isolate infected systems: Immediately disconnect affected devices from the network to prevent further spread.
2. Identify the payload and entry point: Investigate the ransomware strain and analyze logs to pinpoint the attack vector.
3. Assess data impacted: Determine what data was encrypted and if backups are available for restoring critical information.

4. Notify stakeholders: Inform key personnel and authorities according to your incident response plan.
5. Prepare for recovery: If restoring from backups is feasible, ensure their validity and initiate the restoration process.

70. You suspect a coworker might be accessing unauthorized data. What are your initial steps to investigate and address the situation?

The initial steps to investigate and address the situation are as follows:

1. Document your observations: Note specific behaviors, data accessed, and timestamps without directly accusing the individual.
2. Report your concerns to your supervisor or designated security personnel: Follow established internal reporting procedures.
3. Cooperate with the investigation: Offer any relevant information and assist with collecting evidence ethically and discreetly.
4. Maintain confidentiality: Avoid discussing the situation with others before official inquiries conclude.

71. You receive a suspicious email claiming to be from a vendor you regularly work with. How would you determine its legitimacy and avoid falling victim to a phishing attack?

Here are some ideas to determine its legitimacy and avoid falling victim to a phishing attack:

1. Verify sender details: Check the email address and domain name for inconsistencies with the vendor's usual communication.
2. Hover over links without clicking: Preview links to see if they redirect to the expected vendor website.

3. Contact the vendor directly: Use trusted phone numbers or websites to confirm the email's authenticity.
4. Report the attempt: Report the suspicious email to your IT security team for further investigation.

72. You detect unusual activity on your company's cloud storage platform. How do you identify and respond to the potential security incident?

The following steps will help identify and respond to the potential security incident:

1. Analyze logs and audit trails: Identify the nature of the activity, affected files, and potential access points.
2. Utilize cloud security tools: Leverage platform-specific features for threat detection, isolation, and investigation.
3. Engage cloud security support: Collaborate with the cloud provider's security team for advanced analysis and remediation.
4. Notify internal stakeholders: Inform relevant teams about the incident and keep them updated on the response progress

73. Your company website experiences a sudden surge in traffic, potentially indicating a DoS attack. What are your initial steps to mitigate the impact?

The initial steps to mitigate the impact are:

1. Identify the attack type and source: Utilize security tools to analyze traffic patterns and identify the attackers.
2. Activate mitigation strategies: Implement pre-configured DoS protection measures or seek assistance from your security provider.
3. Communicate with users: Inform customers and stakeholders about the attack and any potential service disruptions.

4. Analyze and improve incident response: Evaluate the attack methods and update your defense strategies for future prevention.

MCQs on Cyber Security

74. What is the difference between a virus and a worm?

A. Viruses need a host program to run, while worms can replicate on their own.
B. Worms are always more destructive than viruses.
C. Viruses are always written in assembly language, while worms are written in higher-level languages.
D. There is no difference between a virus and a worm.

Viruses need a host program to run, while worms can replicate on their own.

75. What is a denial-of-service (DoS) attack?

A. A type of attack that tries to steal data
B. A type of attack that tries to crash a website or system
C. A type of attack that tries to trick users into revealing personal information
D. A type of attack that tries to encrypt data

A type of attack that tries to crash a website or system. A DoS attack floods a website or system with traffic, making it unavailable to legitimate users.

76. What is the primary function of an intrusion detection system (IDS)?

A. To prevent unauthorized access to computer systems.
B. To detect and monitor suspicious activity within a network or system.

C. To encrypt data and protect it from unauthorized decryption.
D. To back up data and restore it in case of a cyberattack.

An IDS monitors network traffic and system activity for signs of malicious behavior, alerting security personnel to potential threats.

77. What is the most effective way to protect yourself from social engineering attacks like phishing?

A. Install antivirus software and keep it updated.
B. Be cautious about clicking on links or opening attachments in emails, even from seemingly familiar senders.
C. Never share your personal information online, even on social media.
D. All of the above.

All of the above. Maintaining vigilance, being cautious with links and attachments, and protecting personal information are crucial for avoiding social engineering traps.

78. Which cryptographic algorithm provides the highest level of security for data at rest, making it suitable for highly sensitive information?

A. AES-256
B. RSA-2048
C. SHA-256
D. MD5

RSA-2048 (Image of RSA-2048 encryption)

79. What is the primary benefit of adopting a zero-trust security model compared to traditional perimeter-based defenses?

A. Reduced reliance on firewalls and intrusion detection systems.
B. Continuous authentication and authorization for all users and devices.
C. Enhanced network segmentation and access control policies.
D. Simplified security administration and reduced operational costs.

Continuous authentication and authorization for all users and devices. (Image of Zero Trust security model diagram)

Cyber Security Salary Trends

In India, the average base salary is ₹5,99,180 per year, according to Glassdoor. The average annual salary for a cyber security professional in the US stands at $106,000, with top roles exceeding $200,000.

India:

- Entry-Level: ₹300,000 – ₹400,000
- Senior Management: ₹20 lakh+.
- Average Salary: ₹600,000 per annum (approx. $7,500), but varies based on factors like experience and location

US:

- Entry-Level: $70,000
- Experienced Professionals: $178,000
- Average Salary: $88,325 – $164,861 per year

Cyber Security Job Trends

Cyber security jobs are booming, set to grow 33% by 2030, according to the Bureau of Labor Statistics—way faster than average. Skills that are in demand include cloud security, incident response, data security, and threat intelligence.

1. With more than 200,000 active jobs in the field of cyber security, the tally is expected to increase by 30% in the coming years.
2. With the increase in cyber security remote jobs, it gets more flexible for both companies and working professionals.
3. As the field expands, specializing in areas like threat analysis, forensics, or ethical hacking is becoming increasingly valuable.

Cyber Security Roles and Responsibilities

Type of Cyber Security Role:

With the increasing threat of cyber attacks, cyber security jobs are always in demand. Below are some of the core roles for Cyber Security Professionals.

- Security Engineer
- Information Security Analyst
- Chief information security officer
- Security Architect
- Security Consultant
- Penetration test
- Security Administrator
- Security Manager
- Ethical hacker

Key Cyber Security Responsibilities:

- Monitor network activity, investigate security incidents, and implement security controls.
- Design, implement, and manage security infrastructures and solutions.
- Perform simulated cyber attacks to identify vulnerabilities in systems and networks.
- Develops and oversees the overall security architecture of an organization.
- Leads and manages the organization's overall cybersecurity strategy and posture.

Conclusion

I hope this set of Cyber Interview Questions will help you prepare for your interviews. Best of luck!

If you have any questions, post your queries at intellipaat community space or let us know in the comments, and we'll get back to you.