**🔐✨ Cyber Security Interview Questions for Freshers**

**By: Anu Pasupuleti** 👩‍💻🛡️

🚀 Starting your career in cybersecurity? Here's a quick guide to **top interview questions** that can help you crack your first job! 💼🎯

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from cyber threats like hackers, viruses, and data breaches.

1. What are the common Cyberattacks?

Some basic Cyber-attacks are as follows:

Phishing: Phishing is the fraudulent practice of sending spam emails by impersonating legitimate sources.

Social Engineering Attacks: Social engineering attacks can take many forms and can be carried out anywhere human collaboration is required.

Ransomware: Ransomware is documented encryption programming that uses special cryptographic calculations to encrypt records in a targeted framework.

Cryptocurrency Hijacking: As digital currencies and mining become more popular, so do cybercriminals. They have found an evil advantage in cryptocurrency mining, which involves complex calculations to mine virtual currencies such as Bitcoin, Ethereum, Monero, and Litecoin.

Botnet Attacks: Botnet attacks often target large organizations and entities that obtain vast amounts of information. This attack allows programmers to control countless devices in exchange for cunning intent.

For more details please refer to the article: Types of Cyber Attacks

2. What are the elements of cyber security?

There are various elements of cyber security as given below:

Application Security: Application security is the most important core component of cyber security, adding security highlights to applications during the improvement period to defend against cyber attacks.

Information Security: Information security is a component of cyber security that describes how information is protected against unauthorized access, use, disclosure, disruption, alteration, or deletion.

Network Security: Network security is the security provided to a network from unauthorized access and threats. It is the network administrator's responsibility to take precautions to protect the network from potential security threats. Network security is another element of IT security, the method of defending and preventing unauthorized access to computer networks.

Disaster Recovery Planning: A plan that describes the continuity of work after a disaster quickly and efficiently is known as a disaster recovery plan or business continuity plan. A disaster recovery methodology should start at the business level and identify applications that are generally critical to carrying out the association's activities.

Operational Security: In order to protect sensitive data from a variety of threats, the process of allowing administrators to see activity from a hacker's perspective is called operational security (OPSEC)n or procedural security.

End User Education: End-user training is the most important component of computer security. End users are becoming the number one security threat to any organization because they can happen at any time. One of the major errors that lead to information corruption is human error. Associations must prepare their employees for cyber security.

For more details please refer to the article: Elements of Cybersecurity

3. Define DNS?

The Domain Name System (DNS) translates domain names into IP addresses that browsers use to load web pages. Every device connected to the Internet has its own IP address, which other devices use to identify it in simple language, we can say that DNS Defines the Service of the network.

To know more please refer to the article: Domain Name System (DNS) in Application Layer

4. What is a Firewall?

A firewall is a hardware or software-based network security device that monitors all incoming and outgoing traffic and accepts, denies, or drops that particular traffic based on a defined set of security rules.

Please refer to the article: Introduction of Firewall to know more about this topic.

5. What is a VPN?

VPN stands for Virtual Private Network. A virtual private network (VPN) is a technology that creates a secure, encrypted connection over an insecure network like the Internet. A virtual private network is a method of extending a private network using a public network such as the Internet. The name only indicates that it is a virtual "private network". A user may be part of a local area network at a remote location. Create a secure connection using a tunnelling protocol.

Please refer to the article: Virtual Private Network (VPN) to learn more about this topic.

6. What are the different sources of malware?

The different sources of malware are given below:

Worms: A worm is basically a type of malicious malware that spreads rapidly from one computer to another via email and file sharing. Worms do not require host software or code to execute.

Spyware: Spyware is basically a type of malicious malware that runs in the background of your computer, steals all your sensitive data, and reports this data to remote attackers.

Ransomware: Ransomware is used as malware to extort money from users for ransom by gaining unauthorized access to sensitive user information and demanding payment to delete or return that information from the user.

Virus: A virus is a type of malicious malware that comes as an attachment with a file or program. Viruses usually spread from one program to another program, and they will run only when the host file gets executed. The virus can only cause damage to the computer until the host file runs.

Trojan: Trojans are malicious, non-replicating malware that often degrades computer performance and efficiency. Trojans have the ability to leak sensitive user information and modify and delete this data.

Adware: Adware is another type of malware that tracks the usage of various types of programs and files on your computer and displays personalized ad recommendations based on your usage history.

Please refer to the article: Different Sources of Malware to learn more about this topic.

7. How does email work?

When a sender uses an e-mail program to send an e-mail, it is redirected to a simple e-mail transfer protocol. In this protocol, the recipient's email address belongs to a different domain name or the same domain name as the sender (Gmail, Outlook, etc.). After that, the e-mail will be stored on the server, and later he will send it using the POP or IMAP protocol. Then, if the recipient has a different domain name address, the SMTP protocol communicates with the DNS (Domain Name Server) for the different addresses that the recipient uses. Then the sender's SMTP communicates with the receiver's SMTP, and the receiver's SMTP performs the communication. This way the email is delivered to the recipient's SMTP. If certain network traffic issues prevent both the sender's SMTP and the recipient's SMTP from communicating with each other, outgoing emails will be queued at the recipient's SMTP and finally to be received by the recipient. Also, if a message stays in the queue for too long due to terrible circumstances, the message will be returned to the sender as undelivered.

Please refer to the article: Working of Email to learn more about this topic.

8. What is the difference between active and passive cyber-attacks?

Active Cyber Attack: An active attack is a type of attack in which the attacker modifies or attempts to modify the content of the message. Active attacks are a threat to integrity and availability. Active attacks can constantly corrupt the system and modify system resources. Most importantly, if there is an active attack, the victim is notified of the attack.

Passive Cyber Attack: A passive attack is a type of attack in which the attacker observes the message content or copies the message content. Passive attacks are a threat to confidentiality. Since it is a passive attack, there is no damage to the system. Most importantly, when attacking passively, the victim is not notified of the attack.

Please refer to the article: Difference between Active Attack and Passive Attack to know more about it.

9. What is a social engineering attack?

Social engineering is the act of manipulating individuals to take actions that may or may not be in the best interests of the "target". This may include obtaining information, obtaining access, or obtaining a goal to perform a particular action. It has the ability to manipulate and deceive people. A phone call accompanied by a survey or a quick internet search can bring up dates of birthdays and anniversaries and arm you with that information. This information is enough to create a password attack list.

Please refer to the article: Social Engineering to know more.

10. Who are black hat hackers and white hat hackers?

White Hat Hacker: A white hat hacker is a certified or certified hacker who works for governments and organizations by conducting penetration tests and identifying cybersecurity gaps. It also guarantees protection from malicious cybercrime.

Black Hat Hackers: They are often called crackers. Black hat hackers can gain unauthorized access to your system and destroy your important data. The attack method uses common hacking techniques learned earlier. They are considered criminals and are easy to identify because of their malicious behavior.

Please refer to the article: Types of Hackers to know more.

11. Define encryption and decryption?

Encryption is the process of transforming an ordinary message (plaintext) into a meaningless message (ciphertext). Decryption is the process of transforming a meaningless message (ciphertext) into its original form (plaintext). The main difference between covert writing and covert writing is that it converts the message into a cryptic format that cannot be deciphered unless the message is decrypted. Covert writing, on the other hand, is reconstructing the original message from the encrypted information.

Please refer to the article: Difference between Encryption and Decryption to know more.

12. What is the difference between plaintext and cleartext?

The plaintext is not encrypted at all and cannot be considered encrypted and Clear text is a text sent or stored that has not been encrypted and was not intended to be encrypted. So you don't need to decrypt to see the plaintext. In its simplest form.

13. What is a block cipher?

Block Cipher Converts plaintext to ciphertext using one block of plaintext at a time. Use 64-bit or 64-bit or greater. The complexity of block ciphers is simple. The algorithm modes used in block ciphers are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).

Please refer to the article: Difference between Block Cipher and Stream Cipher to know more.

14. What is the CIA triangle?

When it comes to network security, the CIA Triad is one of the most important models developed to guide information security policy within an organization.

CIA stands for:

Confidentiality

Integrity

availability

Please refer to the article: CIA Triad in Cryptography to know more.

15. What is the Three-way handshake?

TCP uses a three-way handshake to establish reliable connections. The connection is full-duplex, with synchronization (SYN) and acknowledgment (ACK) on both sides. The exchange of these four flags is done in three steps: SYN, SYN to ACK, and ACK.

Please refer to the article: TCP 3-Way Handshake to know more about it.

16. How can identity theft be prevented?

Steps to prevent identity theft:

Use a strong password and don't share her PIN with anyone on or off the phone.

Use two-factor notifications for email. Protect all your devices with one password.

Do not install software from the Internet. Do not post confidential information on social media.

When entering a password with a payment gateway, check its authenticity.

Limit the personal data you run. Get in the habit of changing your PIN and password regularly.

Do not give out your information over the phone.

Please refer to the article: Cyber Crime – Identity Theft to know more about it.

17. What are some common Hashing functions?

The hash function is a function that converts a specific numerical key or alphanumeric key into a small practical integer value. The mapped integer value is used as an index for hash tables. Simply put, a hash function maps any valid number or string to a small integer that can be used as an index into a hash table. The types of Hash functions are given below:

Division Method.

Mid Square Method.

Folding Method.

Multiplication Method.

Please refer to the article Hash Functions to know more about this topic.

18. What do you mean by two-factor authentication?

Two-factor authentication refers to using any two independent methods from a variety of authentication methods. Two-factor authentication is used to ensure users have access to secure systems and to enhance security. Two-factor authentication was first implemented for laptops due to the basic security needs of mobile computing. Two-factor authentication makes it more difficult for unauthorized users to use mobile devices to access secure data and systems.

Please refer to the article Two-factor Authentication to learn more about this topic.

19. What does XSS stand for? How can it be prevented?

Cross-site scripting (XSS) is a vulnerability in web applications that allows third parties to execute scripts on behalf of the web application in the user's browser. Cross-site scripting is one of the most prevalent security vulnerabilities on the Internet today. Exploiting her XSS against users can have a variety of consequences, including Account compromise, account deletion, privilege escalation, malware infection, etc. Effective prevention of XSS vulnerabilities requires a combination of the following countermeasures:

Filter entrance on arrival. As user input comes in, filter expected or valid input as closely as possible. Encode the data on output. When user-controllable data is emitted in an HTTP response, encode the output so that it is not interpreted as active content.

Depending on the output context, it may be necessary to apply a combination of HTML, URL, JavaScript, and CSS encoding. Use proper response headers.

To prevent XSS in HTTP responses that should not contain HTML or JavaScript, use the Content-Type and X-Content-Type-Options headers to force the browser to interpret the response as intended. Content Security Policy. As a last line of defence, a Content Security Policy (CSP) can be used to mitigate the severity of remaining XSS vulnerabilities.

Please refer to the article Cross-Site Scripting (XSS) to learn more about this topic.

20. What do you mean by Shoulder Surfing?

A shoulder surfing attack describes a situation in which an attacker can physically look at a device's screen or keyboard and enter passwords to obtain personal information. Used to - access malware. Similar things can happen from nosy people, leading to an invasion of privacy.

21. What is the difference between hashing and encryption?

| Hashing | Encryption |
| --- | --- |
| This is the process of transforming information into short, fixed values ​​called keys that are used to represent the original information. | This is the process of securely encoding data so that only authorized users who know the key or password can retrieve the original data. |
| The purpose of hashing is to index and retrieve items from the database. The process is very fast. | The purpose of encryption is to transform data and keep it secret from others. |
| There is no way to convert the hash code or key back to the original information. Only mapping is possible, the hash code is checked if the hash code is the same, and the information is checked if the information is the same, otherwise, it is not checked. Original information is not available | If you know the cryptographic key and algorithm used for encryption, you can easily retrieve the original information. |
| It generally tries to generate a new key for each piece of information passed to the hash function, but in rare cases, it can generate the same key, commonly known as a collision. | A new key is always generated for each piece of information. |
| Hashed information is generally small and fixed in length. It does not increase even if the information length of the information increases. | The length of encrypted information is not fixed. It increases |

22. Differentiate between Information security and information assurance.

Information Assurance: It can be described as the practice of protecting and managing risks associated with sensitive information throughout the process of data transmission, processing, and storage. Information assurance primarily focuses on protecting the integrity, availability, authenticity, non-repudiation, and confidentiality of data within a system. This includes physical technology as well as digital data protection.

Information security: on the other hand, is the practice of protecting information by reducing information risk. The purpose is usually to reduce the possibility of unauthorized access or illegal use of the data. Also, destroy, detect, alter, examine, or record any Confidential Information. This includes taking steps to prevent such incidents. The main focus of information security is to provide balanced protection against cyber-attacks and hacking while maintaining data confidentiality, integrity, and availability.

Please refer to the article Information Assurance vs. Information Security to learn more about this topic.

23. Write a difference between HTTPS and SSL.

HTTPS

SSL

It is called Hypertext Transfer Protocol Secure. It is called Secured Socket Layer

This is a more secure version of the HTTP protocol with more encryption capabilities. It is the one and only cryptographic protocol in computer networks.

HTTPS is created by combining the HTTP protocol and SSL. SSL can be used for encryption.

HTTPS is primarily used by websites for logging into banking details and personal accounts. SSL cannot be used alone for a particular website. Used for encryption in conjunction with the HTTP protocol.

HTTPS is the most secure and latest version of the HTTP protocol available today. SSL is being phased out in favour of TLS (Transport Layer Security).

Please refer to the article SSL vs. HTTPS to learn more about this topic.

24. What do you mean by System Hardening?

The attack surface includes all flaws and vulnerabilities that a hacker could use to gain access to your system, such as default passwords, improperly configured firewalls, etc. The idea of ​​system hardening is to make a system more secure by reducing the attack surface present in the design of the system. System hardening is the process of reducing a system's attack surface, thereby making it more robust and secure. This is an integral part of system security practices.

Please refer to the article System Hardening to learn more about this topic.

25. Differentiate between spear phishing and phishing.

Phishing: This is a type of email attack in which an attacker fraudulently attempts to discover a user's sensitive information through electronic communications, pretending to be from a relevant and trusted organization. The emails are carefully crafted by the attackers, targeted to specific groups, and clicking the links installs malicious code on your computer.

Spear phishing: Spear phishing is a type of email attack that targets specific individuals or organizations. In Spear, a phishing attacker tricks a target into clicking a malicious link and installing malicious code, allowing the attacker to obtain sensitive information from the target's system or network.

Please refer to the article Phishing and Spear Phishing to learn more about this topic.

26. What do you mean by Perfect Forward Secrecy?

Perfect Forward Secrecy is a style of encryption that creates a temporary exchange of secret keys between the server and client. It is primarily used to call apps, websites, and messaging apps where user privacy is paramount. A new session key is generated each time the user performs an action. This keeps your data uncompromised and safe from attackers. This is separate from special keys. The basic idea behind Perfect Forward Secrecy technology is to generate a new encryption key each time a user initiates a session. So, if only the encryption key is compromised, the conversation is leaked, and if the user's unique key is compromised, the conversation will continue. Encryption keys generated by Perfect Forward Secrecy keep you safe from attackers. Essentially, it provides double protection from attackers.

Please refer to the article Perfect Forward Secrecy to learn more about this topic.

27. How to prevent MITM?

Strong WEP/WAP Encryption on Access Points

Strong Router Login Credentials Strong Router Login Credentials

Use Virtual Private Network.

Please refer to the article How to Prevent Man In the Middle Attack? to learn more about this topic.

28. What is ransomware?

Ransomware is a type of malware that encrypts data to make it inaccessible to computer users. Cybercriminals use it to extort money from the individuals and organizations that hacked the data and hold the data hostage until a ransom is paid.

Please refer to the article: Ransomware to know more about this.

29. What is Public Key Infrastructure?

A Public Key Infrastructure, or PKI, is the governing authority behind the issuance of digital certificates. Protect sensitive data and give users and systems unique identities. Therefore, communication security is ensured. The public key infrastructure uses keys in public-private key pairs to provide security. Public keys are vulnerable to attacks, so maintaining public keys requires a healthy infrastructure.

Please refer to the article: Public Key Infrastructure to know more.

30. What is Spoofing?

Spoofing is a type of attack on computing devices in which an attacker attempts to steal the identity of a legitimate user and pretend to be someone else. This type of attack is performed to compromise system security or steal user information.

Types of Spoofing:

IP Spoofing: IP is a network protocol that allows messages to be sent and received over the Internet. Her IP address of the sender is included in the message header of all emails sent to her messages (sender address).

ARP Spoofing: ARP spoofing is a hacking technique that redirects network traffic to hackers. Spying on LAN addresses in both wired and wireless LAN networks is called ARP spoofing.

Email Spoofing: Email spoofing is the most common form of identity theft on the Internet. Phishers use official logos and headers to send emails to many addresses impersonating bank, corporate, and law enforcement officials.

Please refer to the article: What is Spoofing? to know more.

Cyber Security Interview Questions for Intermediate

31. What are the steps involved in hacking a server or network?

The following steps must be ensured in order to hack any server or network:

Access your web server.

Use anonymous FTP to access this network to gather more information and scan ports.

Pay attention to file sizes, open ports, and processes running on your system.

Run a few simple commands on your web server like "clear cache" or "delete all files" to highlight the data stored by the server behind these programs. This helps in obtaining more sensitive information that can be used in application-specific exploits.

Connect to other sites on the same network, such as Facebook and Twitter, so that you can check the deleted data. Access the server using the conversion channel.

Access internal network resources and data to gather more information.

Use Metasploit to gain remote access to these resources.

To know more about this topic please refer to the article: How to Hack a Web Server?

32. What are the various sniffing tools?

Lists of some main Networking Sniffing Tools:

Auvik

SolarWinds Network Packet Sniffer

Wireshark

Paessler PRTG

ManageEngine NetFlow Analyzer

Tcpdump

WinDump

NetworkMiner

Please refer to the article: Sniffing Tools to learn more about sniffing tools in ethical hacking.

33. What is SQL injection?

SQL injection is a technique used to exploit user data through web page input by injecting SQL commands as statements. Essentially, these instructions can be used by a malicious user to manipulate her web server for your application. SQL injection is a code injection technique that can corrupt your database. Preventing SQL Injection is given below:

Validation of user input by pre-defining user input length, type, input fields, and authentication.

Restrict user access and determine how much data outsiders can access from your database. Basically, you shouldn't give users permission to access everything in your database.

Do not use system administrator accounts.

To know more about this topic, Please read the article: SQL Injection

34. What is a Distributed Denial of Service attack (DDoS)?

A denial of service (DoS) is a cyber attack against an individual computer or website aimed at denying service to intended users. Its purpose is to interfere with the organization's network operations by denying her access. Denial of service is usually achieved by flooding the target machine or resource with excessive requests, overloading the system, and preventing some or all legitimate requests from being satisfied.

Please refer to the article: Denial of Service and Prevention to know more.

35. How to avoid ARP poisoning?

Following are the five ways of avoiding ARP Poisoning attacks:

Static ARP Tables: If you can verify the correct mapping of MAC addresses to IP addresses, half the problem is solved. This is doable but very costly to administer. ARP tables to record all associations and each network change are manually updated in these tables. Currently, it is not practical for an organization to manually update its ARP table on every host.

Switch Security: Most Ethernet switches have features that help mitigate ARP poisoning attacks. Also known as Dynamic ARP Inspection (DAI), these features help validate ARP messages and drop packets that indicate any kind of malicious activity.

Physical Security: A very simple way to mitigate ARP poisoning attacks is to control the physical space of your organization. ARP messages are only routed within the local network. Therefore, an attacker may have physical proximity to the victim's network.

Network Isolation: A well-segmented network is better than a regular network because ARP messages have a range no wider than the local subnet. That way, if an attack were to occur, only parts of the network would be affected and other parts would be safe. Attacks on one subnet do not affect devices on other subnets.

Encryption: Encryption does not help prevent ARP poisoning, but it does help reduce the damage that could be done if an attack were to occur. Credentials are stolen from the network, similar to the MiTM attack.

Please refer to the article: How to Avoid ARP Poisoning? to know more.

36. What is a proxy firewall?

The proxy firewall monitors application-level information using a firewall proxy server. A proxy firewall server creates and runs a process on the firewall that mirrors the services as if they were running on the end host.

The application layer has several protocols such as HTTP (a protocol for sending and receiving web pages) and SMTP (a protocol for e-mail messages on the Internet). A proxy server like Web Proxy Server is like a process that mirrors the behavior of the HTTP service. Similarly, the FTP proxy server reflects how his FTP service works.

Please refer to the article: What is a Proxy Firewall? to know more.

37. Explain SSL Encryption.

Secure Socket Layer (SSL) provides security for data transferred between web browsers and servers. SSL encrypts the connection between your web server and your browser, keeping all data sent between them private and immune to attack. Secure Socket Layer Protocols: SSL recording protocol.

Please refer to the article: Secure Socket Layer to know more about it.

38. What do you mean by penetration testing?

Penetration testing is done to find vulnerabilities, malicious content, flaws, and risks. It's done to make the organization’s security system defend the IT infrastructure. It is an official procedure that can be deemed helpful and not a harmful attempt. It is part of an ethical hacking process that specifically focuses only on penetrating the information system.

Please refer to the article Penetration Testing to learn more about this topic.

39. What are the risks associated with public Wi-Fi?

Malware, Viruses, and Worms.

Rogue Networks.

Unencrypted Connections

Network Snooping.

Log-in Credential Vulnerability.

System Update Alerts.

Session Hijacking.

Please refer to the article Risks Associated with Public Wi-Fi to learn more about this topic.

40. Explain the main difference between Diffie-Hellman and RSA.

Diffie-Hellman (DH) algorithm: It is a key exchange protocol that allows two parties to communicate over a public channel and establish a shared secret without sending it over the Internet. DH allows two people to use their public key to encrypt and decrypt conversations or data using symmetric cryptography.

RSA: It is a type of asymmetric encryption that uses two different linked keys. RSA encryption allows messages to be encrypted with both public and private keys. The opposite key used to encrypt the message is used to decrypt the message.

41. Give some examples of asymmetric encryption algorithms.

Asymmetric key cryptography is based on public and private key cryptography. It uses two different keys to encrypt and decrypt messages. More secure than symmetric key cryptography, but much slower.

You need two keys, a public key, and a private key. One for encryption and one for decryption.

The ciphertext size is equal to or larger than the original plaintext.

Slow encryption process.

Used to transfer small amounts of data.

Provides confidentiality, authenticity, and non-repudiation.

Please refer to the article Symmetric and Asymmetric Key Encryption to learn more about this topic.

42. Explain social engineering and its attacks.

Social engineering is a hacking technique based on forging someone's identity and using socialization skills to obtain details. There are techniques that combine psychological and marketing skills to influence targeted victims and manipulate them into obtaining sensitive information. The types of social engineering attacks are given below:

Impersonation: This is a smart choice for attackers. This method impersonates organizations, police, banks, and tax authorities. Then they steal money or anything they want from the victim. And the same goes for organizations that obtain information about victims legally through other means.

Phishing: Phishing is like impersonating a well-known website such as Facebook and creating a fake girlfriend website to trick users into providing account credentials and personal information. Most phishing attacks are carried out through social media such as Instagram, Facebook, and Twitter.

Vishing: Technically speaking, this is called "voice phishing". In this phishing technique, attackers use their voice and speaking skills to trick users into providing personal information. In general, this is most often done by organizations to capture financial and customer data.

Smithing: Smithing is a method of carrying out attacks, generally through messages. In this method, attackers use their fear and interest in a particular topic to reach out to victims through messages. These topics are linked to further the phishing process and obtaining sensitive information about the target.

Please refer to the article Social Engineering: The Attack on Human Brain and Trust to learn more about this topic.

43. State the difference between a virus and worm.

Worms: Worms are similar to viruses, but do not modify the program. It replicates more and more to slow down your computer system. The worm can be controlled with a remote control. The main purpose of worms is to eat up system resources. The 2000 WannaCry ransomware worm exploits the resource-sharing protocol Windows Server Message Block (SMBv1).

Virus: A virus is malicious executable code attached to another executable file that can be harmless or modify or delete data. When a computer program runs with a virus, it performs actions such as B. Delete the file from your computer system. Viruses cannot be controlled remotely. The ILOVEYOU virus spreads through email attachments.

Please refer to the article Difference between Worms and Virus to know more about this topic.

44. Explain the concept of session hijacking.

Session hijacking is a security attack on user sessions over a protected network. The most common method of session hijacking is called IP spoofing, where an attacker uses source-routed IP packets to inject commands into the active communication between two nodes on a network, allowing an authenticated impersonation of one of the users. This type of attack is possible because authentication usually only happens at the beginning of a TCP session. The types of session hijacking are given below:

Packet Sniffing

CSRF (Cross-site Request Forgery)

Cross-site Scripting

IP spoofing

Please refer to the article Session Hijacking to learn more about this topic.

45. Explain the honeypot and its types.

A honeypot is a networked system that acts as a trap for cyber attackers to detect and investigate hacker tactics and types of attacks. Acting as a potential target on the Internet, it notifies defenders of unauthorized access to information systems. Honeypots are classified based on their deployment and intruder involvement. Based on usage, honeypots are classified as follows:

Research honeypots: Used by researchers to analyze hacking attacks and find different ways to prevent them.

Production Honeypots: Production honeypots are deployed with servers on the production network. These honeypots act as a front-end trap for attackers composed of false information, giving administrators time to fix all vulnerabilities in real systems.

Please refer to the article What is Honeypot? to know more about this topic.

46. What do you mean by a Null Session?

Null session attacks have existed since Windows 2000 was widely used. However, system administrators do not consider this type of attack when implementing network security measures. This can have unimaginable consequences, as this type of attack allows hackers to obtain all the information they need to access your system remotely. This type of attack is more difficult to execute if the customer is using a newer version of the operating system, but Windows XP and Windows Server 2003 are still the most common.

Please refer to the article Null Session to learn more about this topic.

47. What is IP blocklisting?

IP blacklisting is a method used to block unauthorized or malicious IP addresses from accessing your network. A blacklist is a list of ranges or individual IP addresses to block.

Please refer to the article What is IP blocklisting? to know more about this topic.

48. What are Polymorphic viruses?

"Poly" refers to many and "morphic" refers to the shape. Thus, polymorphic viruses, as the name suggests, are complex computer viruses that change shape as they spread in order to avoid detection by antivirus programs. This is a self-encrypting virus that combines a mutation engine with a self-propagating code. A polymorphic virus consists of:

Encrypted virus body mutation engine that generates random decryption routines.

A polymorphic virus has its mutation engine and virus body encrypted. When an infected program is run, a virus decryption routine takes control of the computer and decrypts the virus body and mutation engine.

Control is then passed to the virus to detect new programs to infect. Since the body of the virus is encrypted and the decryption routine varies from infection to infection, virus scanners cannot look for a fixed signature or fixed decryption routine, making detection more difficult.

Please refer to the article Polymorphic Viruses to learn more about this topic.

49. What is a Botnet?

A botnet (short for "robot network") is a network of malware-infected computers under the control of a single attacker known as a "bot herder". An individual machine under the control of a bot herder is called a bot.

Please refer to the article Botnet in Computer Networks to learn more about this topic.

50. What is an Eavesdropping Attack?

Eavesdropping occurs when a hacker intercepts, deletes or modifies data sent between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data sent between devices.

Please refer to the article Eavesdropping Attack to learn more about this topic.

Cyber Security Interview Questions for Experienced

51. What is the man-in-the-middle attack?

This is a type of cyber attack in which the attacker stays between the two to carry out their mission. The type of function it can perform is to modify the communication between two parties so that both parties feel like they are communicating over a secure network.

Please refer to the article: Man In the Middle Attack to learn more about this topic.

52. What is a traceroute? Why is it used?

Traceroute is a widely used command line tool available on almost all operating systems. A complete route to the destination address is displayed. It also shows the time (or delay) between intermediate routers.

Uses of traceroute:

It enables us to locate where the data was unable to be sent along

Traceroute helps provide a map of data on the internet from source to destination

It works by sending ICMP (Internet Control Message Protocol) packets.

You can do a visual traceroute to get a visual representation of each hop.

Please refer to the article: Traceroute in Network Layer to know more about it.

53. What is the difference between HIDS and NIDS?

HIDS: This intrusion detection system sees the host itself as a whole world. It can be a computer (PC) or a server that can act as a standalone system and analyze and monitor its own internals. It works by looking at the files/data coming in and out of the host you're working on. It works by taking existing file system snapshots from a previously taken file system and comparing them to each other. If they are the same, it means the host is safe and not under attack, but a change could indicate a potential attack.

NIDS: This system is responsible for installation points across the network and can operate in mixed and hybrid environments. Alerts are triggered when something malicious or anomalous is detected in your network, cloud, or other mixed environments.

Please refer to the article: Difference between HIDs and NIDs to know more about it.

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

Penetration testing: This is performed to find vulnerabilities, malicious content, bugs, and risks. Used to set up an organization's security system to protect its IT infrastructure. Penetration testing is also known as penetration testing. This is an official procedure that can be considered helpful, not a harmful attempt. This is part of an ethical hacking process that focuses solely on breaking into information systems.

Vulnerability assessment: It is the technique of finding and measuring (scanning) security vulnerabilities in a particular environment. This is a location-comprehensive evaluation (result analysis) of information security. It is used to identify potential vulnerabilities and provide appropriate mitigations to eliminate them or reduce them below the risk level.

Please refer to the article: Differences between Penetration Testing and Vulnerability Assessments to know more.

55. What is RSA?

The RSA algorithm is an asymmetric encryption algorithm. Asymmetric means that it actually works with two different keys. H. Public and Private Keys. As the name suggests, the public key is shared with everyone and the private key remains secret.

Please refer to the article: RSA Algorithm in Cryptography to know more.

56. What is the Blowfish algorithm?

Blowfish is an encryption technique developed by Bruce Schneier in 1993 as an alternative to the DES encryption technique. It is considerably faster than DES and provides excellent encryption speed even though no effective cryptanalysis techniques have been discovered so far. It was one of the first secure block ciphers to be patent-free and therefore freely available to everyone.

Block size: 64 bits

keys: variable size from 32-bit to 448-bit

Number of subkeys: 18 [P array]

Number of rounds: 16

Number of replacement boxes: 4 [each with 512 entries of 32 bits]

Please refer to the article: Blowfish Algorithm to know more.

57. What is the difference between a vulnerability and an exploit?

Vulnerability: A vulnerability is an error in the design or implementation of a system that can be exploited to cause unexpected or undesirable behaviour. There are many ways a computer can become vulnerable to security threats. A common vulnerability is for attackers to exploit system security vulnerabilities to gain access to systems without proper authentication.

Exploit: Exploits are tools that can be used to exploit vulnerabilities. They are created using vulnerabilities. Exploits are often patched by software vendors as soon as they are released. They take the form of software or code that helps control computers and steal network data.

Please refer to the article: Difference Between Vulnerability and Exploit to know more about it.

58. What do you understand by Risk, Vulnerability and threat in a network?

Cyber threats are malicious acts aimed at stealing or corrupting data or destroying digital networks and systems. A threat can also be defined as the possibility of a successful cyberattack to gain unethical access to sensitive data on a system.

Vulnerabilities in cybersecurity are deficiencies in system designs, security procedures, internal controls, etc. that can be exploited by cybercriminals. In very rare cases, cyber vulnerabilities are the result of cyberattacks rather than network misconfigurations.

Cyber ​​risk is the potential result of loss or damage to assets or data caused by cyber threats. You can't eliminate risk completely, but you can manage it to a level that meets your organization's risk tolerance. Therefore, our goal is not to build a system without risk but to keep the risk as low as possible.

Please refer to the article: Difference Between Threat, Vulnerability and Risk in Computer Networks to know more.

59. Explain Phishing and how to prevent it.

Phishing is a type of cyber attack. The name phishing comes from the word 'phish', which means fish. Placing bait to catch fish is a common phenomenon. Phishing works similarly. Tricking users or victims into clicking on malicious websites is an unethical practice.

Here's how to protect your users from phishing attacks.

Download software only from authorized sources

Do not share personal information on unknown links.

Always check website URLs to prevent such attacks.

If you receive an email from a known source, but the email seems suspicious, contact the sender with a new email instead of using the reply option.

Avoid posting personal information such as phone numbers, addresses, etc. on social media.

Monitor compromised websites with malicious content using phishing detection tools. Try to avoid free Wi-Fi.

60. What do you mean by Forward Secrecy and how does it work?

Forward secrecy is a feature of some key agreement protocols that guarantees that the session keys will remain secure even if the server's private key is compromised. Perfect forward secrecy, also known as PFS, is the term used to describe this. The "Diffie-Hellman key exchange" algorithm is employed to achieve this.