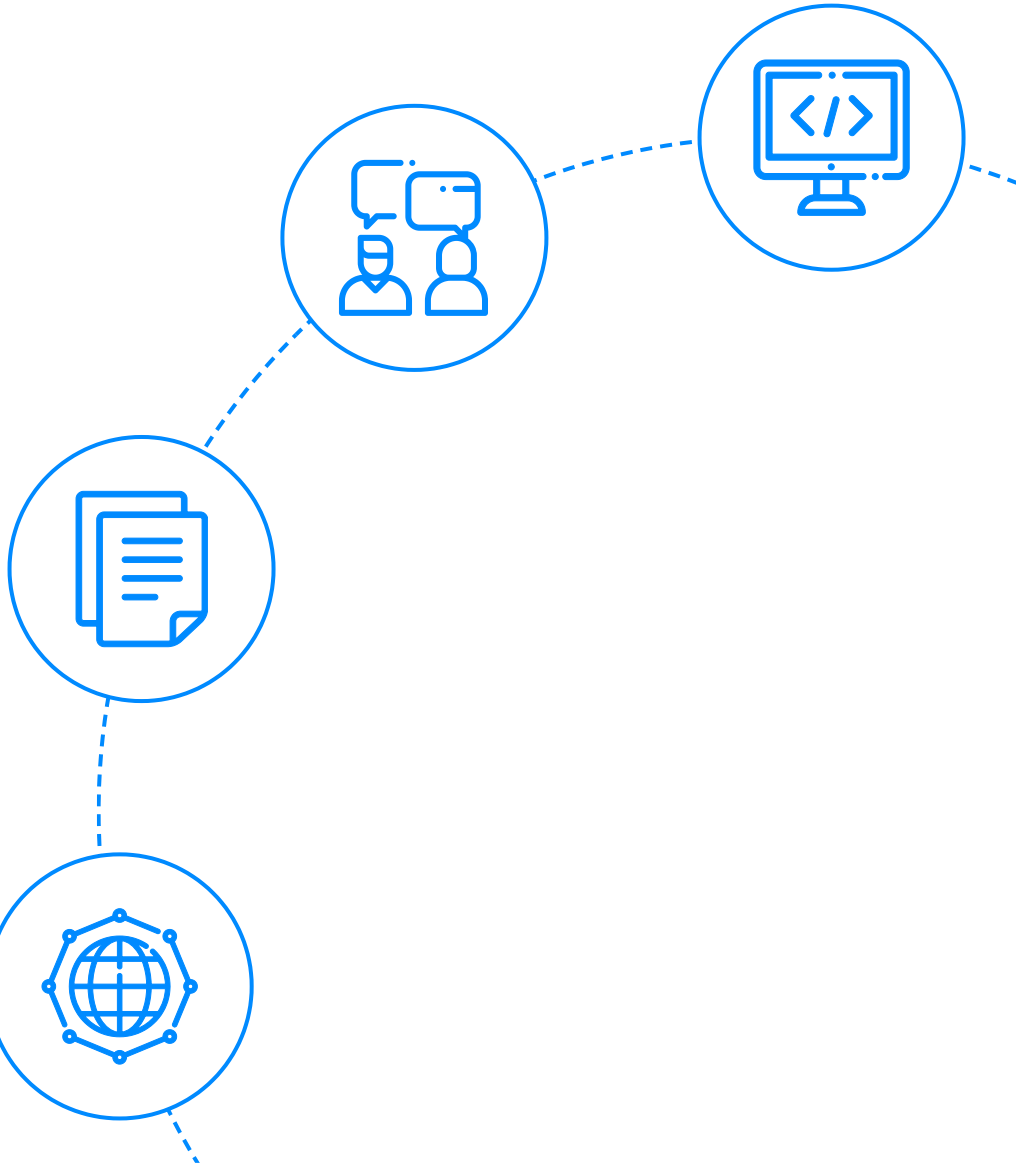
InterviewBit

Cyber Security Interview Questions



To view the live version of the page, click here.

Contents

Cyber Security Interview Questions for Freshers

Cyber Security Interview Questions for Freshers

(.....Continued)

21. Differentiate between Information protection and information assurance.

Cyber Security Interview Questions for Experienced

22. Differentiate between VPN and VLAN.
23. What do you mean by perimeter-based and data-based protection?
24. Which is more reliable: SSL or HTTPS?
25. Differentiate between Symmetric and Asymmetric Encryption.
26. What do you mean by a DDoS attack? How can you prevent it?
27. Differentiate between IDS and IPS in the context of Cyber Security.
28. What do you mean by Network Sniffing?
29. Differentiate between Black Box Testing and White Box Testing.
30. What do you mean by System Hardening?
31. Differentiate between HIDS and NIDS.
32. What do you mean by Domain Name System (DNS) Attack?
33. Differentiate between Stream Cipher and Block Cipher.
34. Differentiate between spear phishing and phishing?
35. What do you mean by ARP poisoning?
36. What do you mean by SQL Injection? How do you prevent it?
37. What is the difference between virus and worm?
38. What form of cookie might be used in a spyware attack?

Cyber Security Interview Questions for Experienced

(.....Continued)

39. How do you decide the placement of the encryption function?
40. What are Polymorphic viruses?
41. What do you mean by Active reconnaissance?
42. What do you mean by Forward Secrecy and how does it work?

Let's get Started

Introduction to Cyber Security:

Cybersecurity is the process of safeguarding internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cybersecurity can be broken down into two subparts: cyber and security. The term "cyber" refers to a wide range of technology, including systems, networks, programs, and data. Security, on the other hand, is concerned with the safeguarding of systems, networks, applications, and data. It's also known as electronic information security or information technology security in some circumstances. Cyber Security" is defined as "a set of technologies, processes, and practices aimed at preventing attacks, theft, damage, modification, or unauthorized access to networks, devices, programs, and data. In other words, Cyber Security is a set of concepts and techniques meant to secure our computing resources and online information against attackers.

Importance of Cyber Security:-

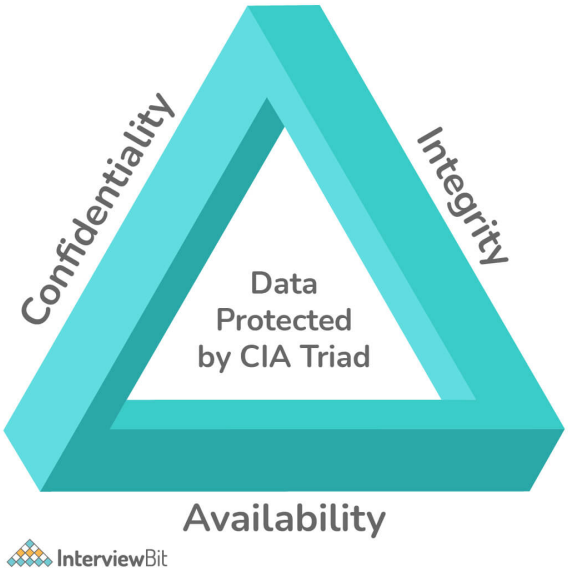
We now live in a digital era in which the internet, computers, and other electronic gadgets, as well as software programs, are integral parts of our daily lives. All vital infrastructures, including the banking system, hospitals, financial institutions, governments, and manufacturing industries, rely on Internet-connected devices to run their businesses. Some of their data, such as intellectual property, financial data, and personal information, is vulnerable to unauthorized access or exposure, which could result in severe consequences. Intruders and threat actors can use this information to penetrate them for financial gain, extortion, political or social reasons, or simply destruction.

Cyber-attacks, which compromise the system, are becoming a global concern, and other security breaches could jeopardize the global economy. As a result, having a strong cybersecurity strategy in place to protect sensitive data from high-profile security breaches is critical. Furthermore, as the number of cyber-attacks rises, businesses and organizations, particularly those dealing with sensitive business and personal information such as national security, health, or financial records, must employ strong cybersecurity measures and processes to protect their sensitive data.

Cyber Security Interview Questions for Freshers

1. What is the main objective of Cyber Security?

The primary goal of cyber security is to protect data. To safeguard data from cyber-attacks, the security sector offers a triangle of three connected principles. The CIA trio is the name for this principle. The CIA model is intended to help organizations develop policies for their information security architecture. One or more of these principles has been broken when a security breach is discovered. Confidentiality, Integrity, and Availability are the three components of the CIA model. It's a security paradigm that guides individuals through many aspects of IT security. Let's take a closer look at each section.



Confidentiality: Confidentiality is the same as privacy in that it prevents unauthorized access to data. It entails ensuring that the data is only accessible to those who are authorized to use it, as well as restricting access to others. It keeps vital information from getting into the wrong hands. Data encryption is a great example of keeping information private.
Integrity: This principle assures that the data is genuine, correct, and safe from unwanted threat actors or unintentional user alteration. If any changes are made, precautions should be taken to protect sensitive data from corruption or loss, as well as to quickly recover from such an incident. Furthermore, it denotes that the source of information must be genuine.
Availability: This principle ensures that information is constantly available and helpful to those who have access to it. It ensures that system failures or cyber-attacks do not obstruct these accesses.

2. Differentiate between threat, vulnerability and risk.

Threat: A threat is any form of hazard that has the potential to destroy or steal data, disrupt operations, or cause harm in general. Malware, phishing, data breaches, and even unethical employees are all examples of threats.
Threat actors, who might be individuals or groups with a variety of backgrounds and motives, express threats. Understanding threats is essential for developing effective mitigations and making informed cybersecurity decisions. Threat intelligence is information regarding threats and threat actors.

Vulnerability: A vulnerability is a flaw in hardware, software, personnel, or procedures that threat actors can use to achieve their objectives.
Physical vulnerabilities, such as publicly exposed networking equipment, software vulnerabilities, such as a buffer overflow vulnerability in a browser, and even human vulnerabilities, such as an employee vulnerable to phishing assaults, are all examples of vulnerabilities.
Vulnerability management is the process of identifying, reporting and repairing vulnerabilities. A zero-day vulnerability is a vulnerability for which a remedy is not yet available.

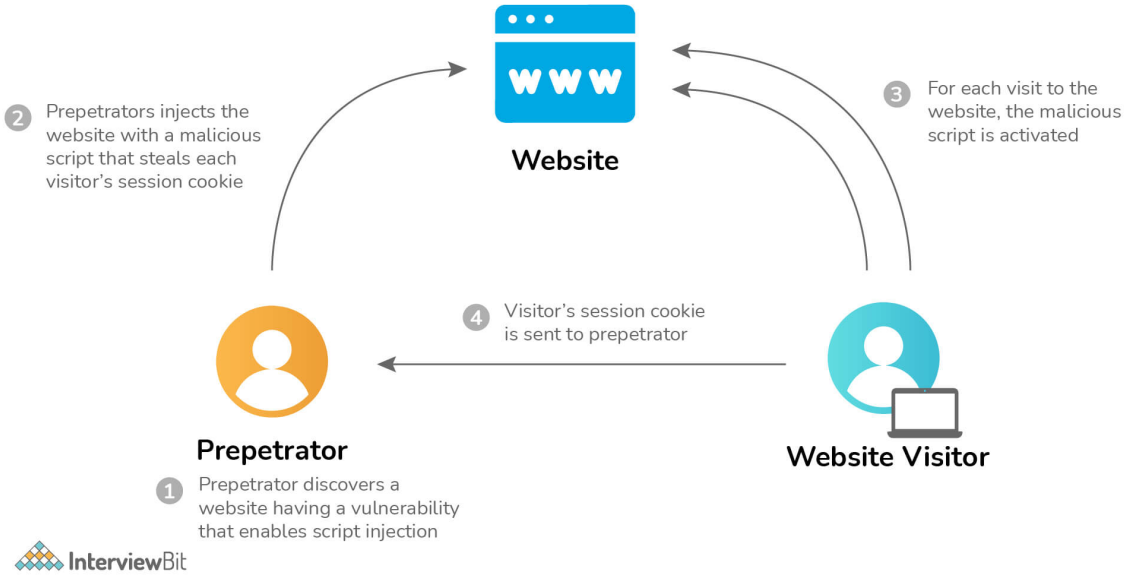
Risk: The probability of a threat and the consequence of a vulnerability are combined to form risk. To put it another way, the risk is the likelihood of a threat agent successfully exploiting a vulnerability, which may be calculated using the formula:

Risk = Likelihood of a threat * Vulnerability Impact

Risk management is the process of identifying all potential hazards, analyzing their impact, and determining the best course of action. It's a never-ending procedure that examines new threats and vulnerabilities on a regular basis. Risks can be avoided, minimized, accepted, or passed to a third party depending on the response chosen.

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

XSS stands for Cross-site scripting. It is a web security flaw that allows an attacker to manipulate how users interact with a susceptible application. It allows an attacker to get around the same-origin policy, which is meant to keep websites separate from one another. Cross-site scripting flaws allow an attacker to impersonate a victim user and execute any actions that the user is capable of, as well as access any of the user's data. If the victim user has privileged access to the application, the attacker may be able to take complete control of the app's functionality and data.



Preventing cross-site scripting can be simple in some circumstances, but it can be much more difficult in others, depending on the application's sophistication and how it handles user-controllable data. In general, preventing XSS vulnerabilities will almost certainly need a mix of the following measures:

On arrival, filter the input. Filter user input as precisely as feasible at the point when it is received, based on what is expected or valid input.

On the output, encode the data. Encode user-controllable data in HTTP responses at the point where it is output to avoid it being perceived as active content. Depending on the output context, a combination of HTML, URL, JavaScript, and CSS encoding may be required.

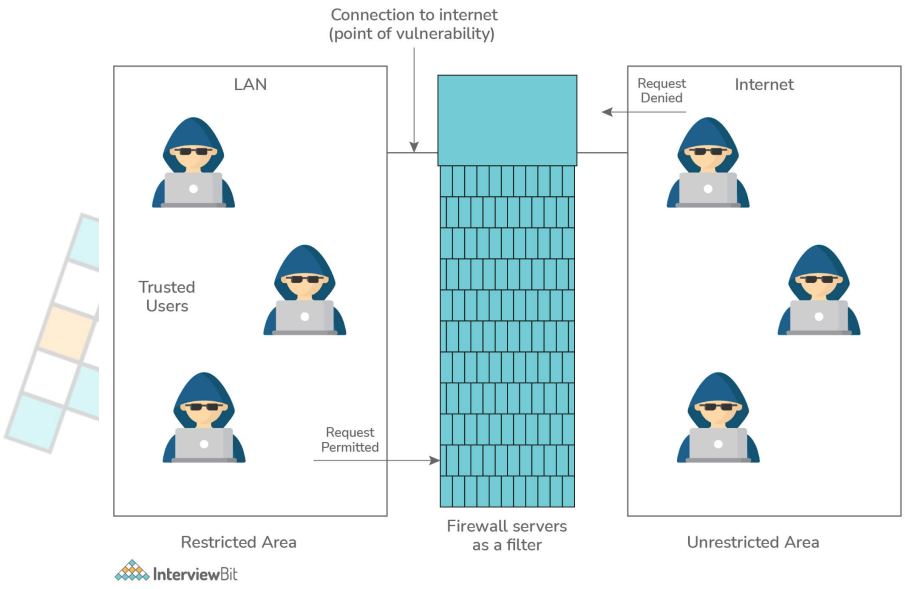
Use headers that are relevant for the response. You can use the Content-Type and X-Content-Type-Options headers to ensure that browsers read HTTP responses in the way you intend, preventing XSS in HTTP responses that aren't intended to contain any HTML or JavaScript.

Policy for Content Security. You can utilize Content Security Policy (CSP) as a last line of defense to mitigate the severity of any remaining XSS issues.

4. What is a Firewall?

A firewall serves as a barrier between a LAN and the Internet. It allows private resources to remain private while reducing security threats. It manages both inbound and outbound network traffic.

A sample firewall between a LAN and the internet is shown in the diagram below. The point of vulnerability is the connection between the two. At this point, network traffic can be filtered using both hardware and software.

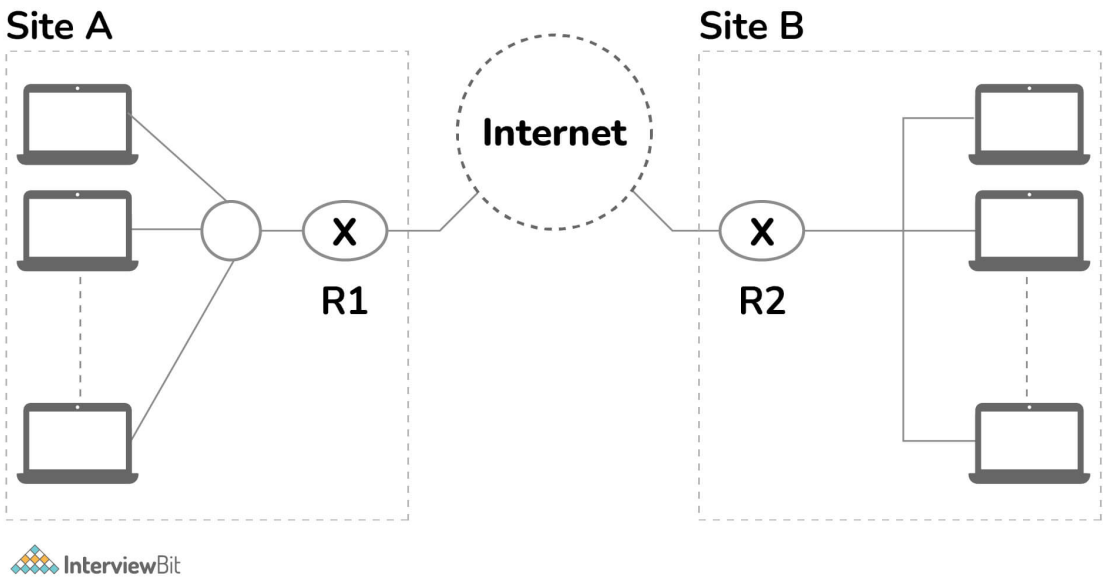


There are two types of firewall systems: one that uses network layer filters and the other that uses user, application, or network layer proxy servers.

5. Define VPN.

The term VPN refers to a virtual private network. It enables you to connect your computer to a private network, establishing an encrypted connection that hides your IP address, allowing you to safely share data and access the web while safeguarding your online identity.

A virtual private network, or VPN, is an encrypted link between a device and a network via the Internet. The encrypted connection aids in the secure transmission of sensitive data. It protects against illegal eavesdropping on the traffic and allows the user to work remotely. In corporate settings, VPN technology is commonly used.



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

Black Hat hackers, sometimes known as crackers, attempt to obtain unauthorized access to a system in order to disrupt its operations or steal critical data.

Because of its malicious aim, black hat hacking is always illegal, including stealing company data, violating the privacy, causing system damage, and blocking network connection, among other things.

Ethical hackers are also referred to as **White hat hackers**. As part of penetration testing and vulnerability assessments, they never intend to harm a system; rather, they strive to uncover holes in a computer or network system.
Ethical hacking is not a crime and is one of the most difficult professions in the IT business. Many businesses hire ethical hackers to do penetration tests and vulnerability assessments.

Grey hat hackers combine elements of both black and white hat hacking. They act without malice, but for the sake of amusement, they exploit a security flaw in a computer system or network without the permission or knowledge of the owner. Their goal is to draw the owners' attention to the flaw in the hope of receiving gratitude or a small reward.

7. What are the types of Cyber Security?

The assets of every company are made up of a variety of various systems. These systems have a strong cybersecurity posture, which necessitates coordinated actions across the board. As a result, cybersecurity can be divided into the following sub-domains:

Network security: It is the process of securing a computer network against unauthorized access, intruders, attacks, disruption, and misuse using hardware and software. This security aids in the protection of an organization's assets from both external and internal threats. Example: Using a Firewall.
Application security: It entails safeguarding software and devices against malicious attacks. This can be accomplished by regularly updating the apps to ensure that they are secure against threats.
Data security: It entails putting in place a strong data storage system that ensures data integrity and privacy while in storage and transport.
Identity management: It refers to the process of identifying each individual's level of access inside an organization. Example: Restricting access to data as per the job role of an individual in the company.
Operational security: It entails analyzing and making decisions about how to handle and secure data assets. Example: Storing data in an encrypted form in the database.
Mobile security: It refers to the protection of organizational and personal data held on mobile devices such as cell phones, PCs, tablets, and other similar devices against a variety of hostile attacks. Unauthorized access, device loss or theft, malware, and other threats are examples of these dangers.
Cloud security: It refers to the safeguarding of data held in a digital environment or in cloud infrastructures for an organization. It employs a variety of cloud service providers, including AWS, Azure, Google, and others, to assure protection against a variety of threats.

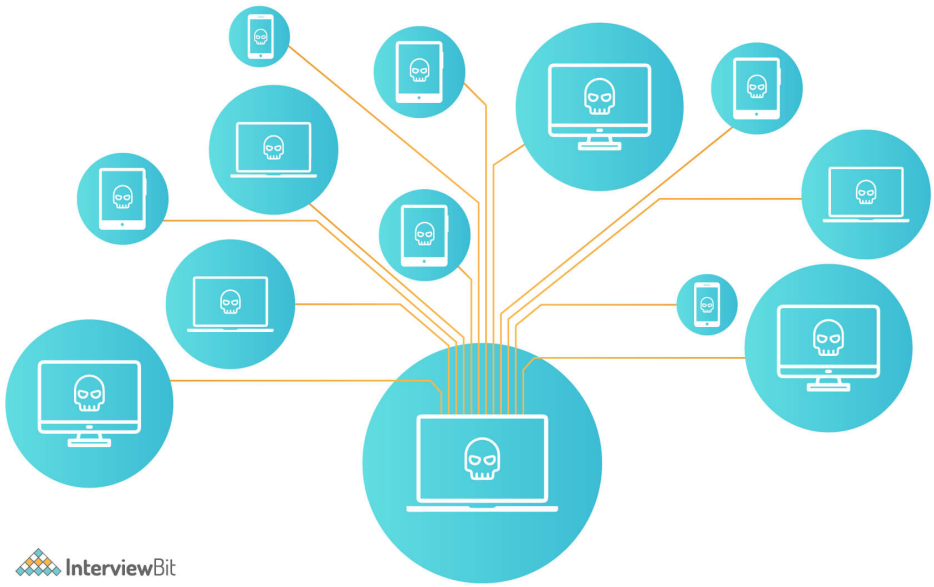
8. What are the benefits of Cyber Security?

The following are some of the advantages of putting cybersecurity in place and keeping it up to date:

- Businesses are protected from cyberattacks and data breaches.
- Both data and network security are safeguarded.
- Unauthorized user access is kept to a minimum.
- There is a quicker recovery time after a breach.
- Protection for end-users and endpoint devices.
- Regulatory compliance.
- Operational consistency.
- Developers, partners, consumers, stakeholders, and employees have a higher level of trust in the company's reputation.

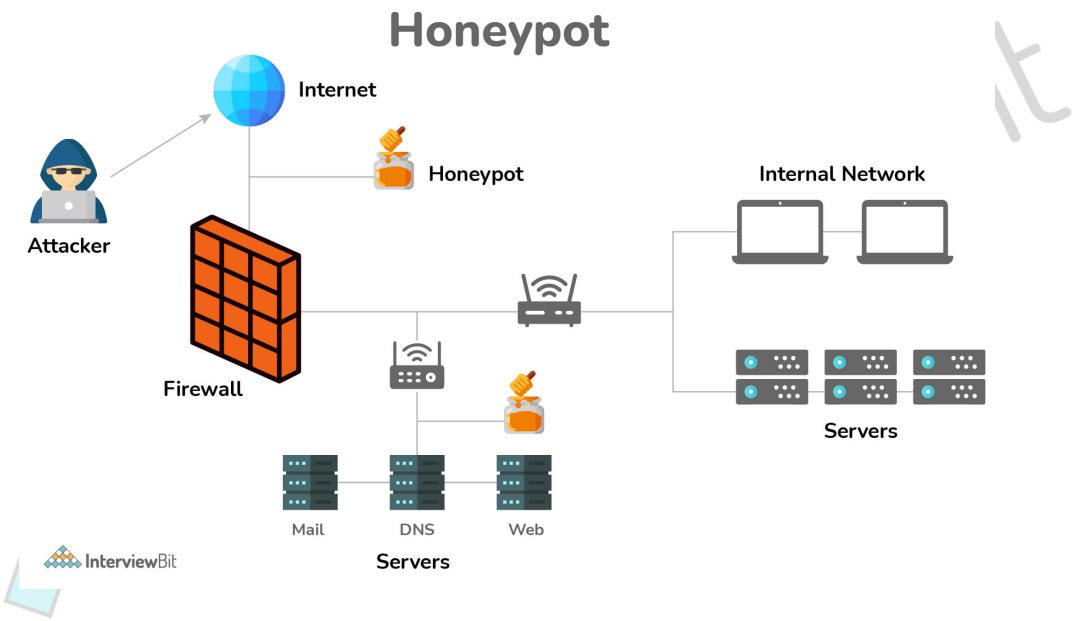
9. What do you mean by a botnet?

A botnet is a collection of internet-connected devices, such as servers, PCs, and mobile phones, that are infected with malware and controlled by it.
It's used to steal data, send spam, launch distributed denial-of-service (DDoS) attacks, and more, as well as provide the user access to the device and its connection.



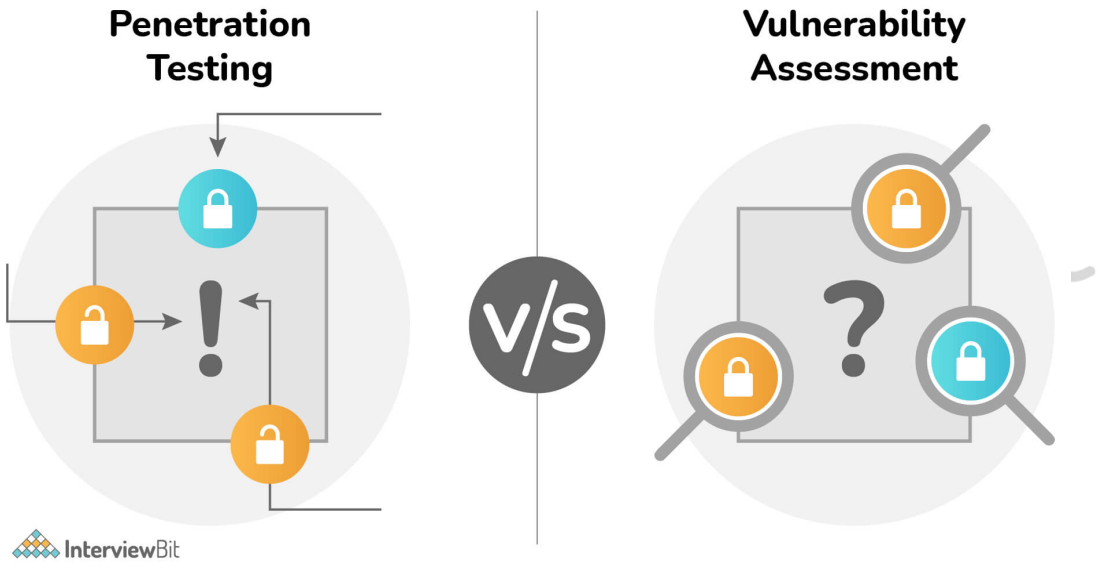
10. What do you mean by honeypots?

Honeypots are attack targets that are set up to see how different attackers attempt exploits. Private firms and governments can utilize the same concept to evaluate their vulnerabilities, which is widely used in academic settings.



11. Differentiate between Vulnerability Assessment and Penetration Testing.

Vulnerability assessment and penetration testing are two different phrases that both serve the same purpose: to secure the network environment.



Vulnerability Assessment is a process for defining, detecting, and prioritizing vulnerabilities in computer systems, network infrastructure, applications, and other systems, as well as providing the necessary information to the organization to correct the flaws.
Penetration Testing is also known as ethical hacking or pen-testing. It's a method of identifying vulnerabilities in a network, system, application, or other systems in order to prevent attackers from exploiting them. It is most commonly used to supplement a web application firewall in the context of web application security (WAF).
A vulnerability scan is similar to approaching a door and checking to see if it is unlocked before stopping. A penetration test goes a step further, not only checking to see if the door is unlocked but also opening the door and walking right in.

12. What do you mean by a Null Session?

A null session occurs when a user is not authorized using either a username or a password. It can provide a security concern for apps because it implies that the person making the request is unknown.

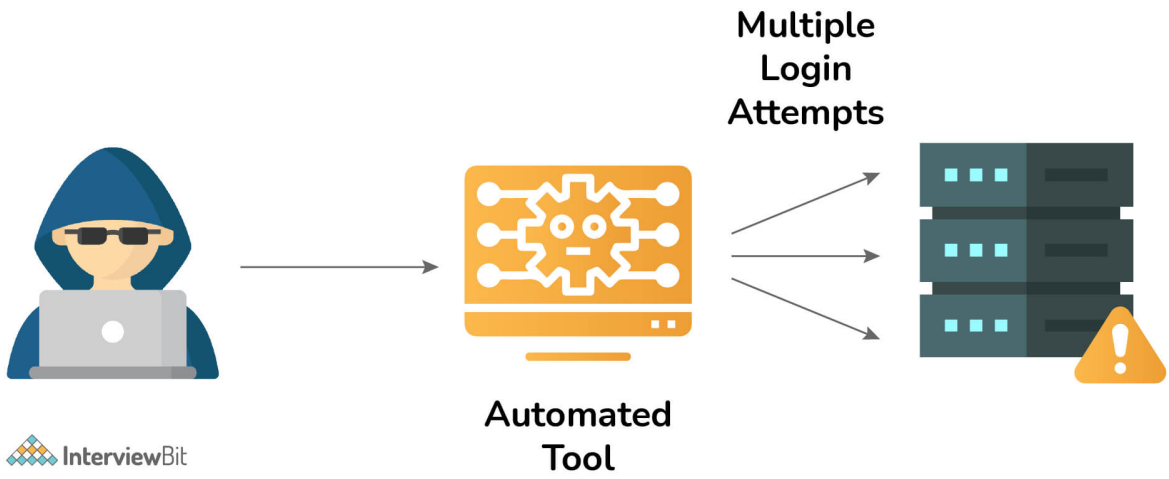
13. What are the common types of cyber security attacks?

The common types of cyber security attacks are:-

- Malware
- Cross-Site Scripting (XSS)
- Denial-of-Service (DoS)
- Domain Name System Attack
- Man-in-the-Middle Attacks
- SQL Injection Attack
- Phishing
- Session Hijacking
- Brute Force

14. What do you mean by brute force in the context of Cyber Security?

A brute force attack is a cryptographic assault that uses a trial-and-error approach to guess all potential combinations until the correct data is discovered. This exploit is commonly used by cybercriminals to gain personal information such as passwords, login credentials, encryption keys, and PINs. It is very easy for hackers to implement this.



15. What do you mean by Shoulder Surfing?

Shoulder surfing is a form of physical assault that entails physically peering at people's screens while they type information in a semi-public space.

16. What do you mean by Phishing?

Phishing is a sort of cybercrime in which the sender appears to be a legitimate entity such as PayPal, eBay, financial institutions, or friends and coworkers. They send an email, phone call, or text message to a target or target with a link to convince them to click on the link. This link will take users to a fake website where they will be asked to enter sensitive information such as personal information, banking and credit card information, social security numbers, usernames, and passwords. By clicking the link, malware will be installed on the target machines, allowing hackers to remotely control them.

You can protect yourself from phishing attacks by following these guidelines:

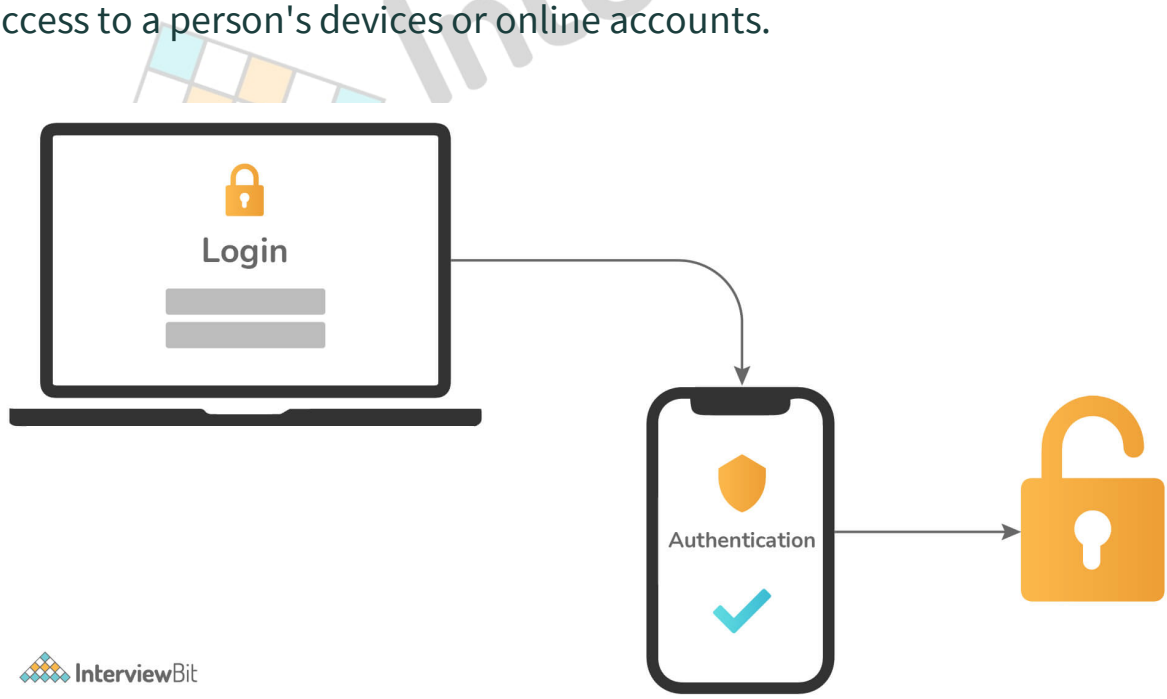
- Don't give out important information on websites you don't know.
- Check the site's security.
- Make use of firewalls.
- Use Toolbar for Anti-Phishing

17. Differentiate between hashing and encryption.

Hashing	Encryption
It is a method of converting data to a smaller fixed value known as the key, which is then used to represent the original data.	It's the technique of securely e that only the authorized user password can get the original else, it seems to be rubbish.
By whatever method, the hash code or key cannot be reverted to the original information. It can only be mapped, and the hash code is compared; if the hash code is the same, the information is identical; otherwise, it is not. It is not possible to get the original data.	If we know the encryption key for encryption, we can easily e data.
In comparison to encryption, it is more secure.	In comparison to hashing, it is
The goal of hashing is to index and retrieve data from a database. The procedure is really quick.	Encryption transforms data in hidden from others.
The hashed data is usually short and constant in length. It does not increase in size as the length of information increases.	The length of the encrypted d expands as the amount of dat
Eg:- SHA256 algorithm	Eg:- RSA, AES algorithm

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

Two-factor authentication (2FA), often known as two-step verification or dual-factor authentication, is a security method in which users validate their identity using two independent authentication factors. This procedure is carried out in order to better protect the user's credentials as well as the resources that the user has access to. Single-factor authentication (SFA), in which the user gives only one factor — generally a password or passcode — provides a lower level of security than two-factor authentication (TFA). Since possessing the defendant's password alone is not enough to accomplish the authentication check, two-factor authentication adds an extra layer of security to the authentication process, making it more difficult for attackers to get access to a person's devices or online accounts.



19. How can you avoid a brute force attack?

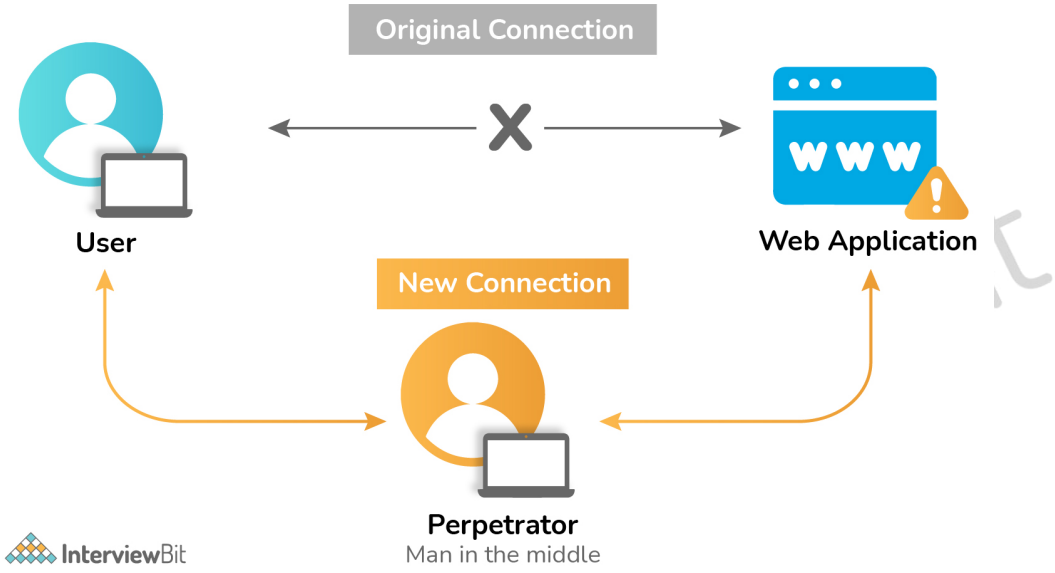
There are a variety of techniques for stopping or preventing brute force attacks.

A robust password policy is the most evident. Strong passwords should be enforced by every web application or public server. Standard user accounts, for example, must contain at least eight characters, a number, uppercase and lowercase letters, and a special character. Furthermore, servers should mandate password updates on a regular basis.
Brute Force attack can also be avoided by the following methods:-

- Limit the number of failed login attempts.
- By altering the sshd_config file, you can make the root user unreachable via SSH.
- Instead of using the default port, change it in your sshd config file.
- Make use of Captcha.
- Limit logins to a certain IP address or range of IP addresses.
- Authentication using two factors
- URLs for logging in that are unique
- Keep an eye on the server logs.

20. What do you mean by Man-in-the-Middle Attack?

A cyber threat (a type of eavesdropping assault) in which a cybercriminal wiretaps a communication or data transmission between two people is known as a man-in-the-middle attack. Once a cybercriminal enters a two-way conversation, they appear to be genuine participants, allowing them to obtain sensitive information and respond in a variety of ways. The main goal of this type of attack is to acquire access to our company's or customers' personal information. On an unprotected Wi-Fi network, for example, a cybercriminal may intercept data passing between the target device and the network.



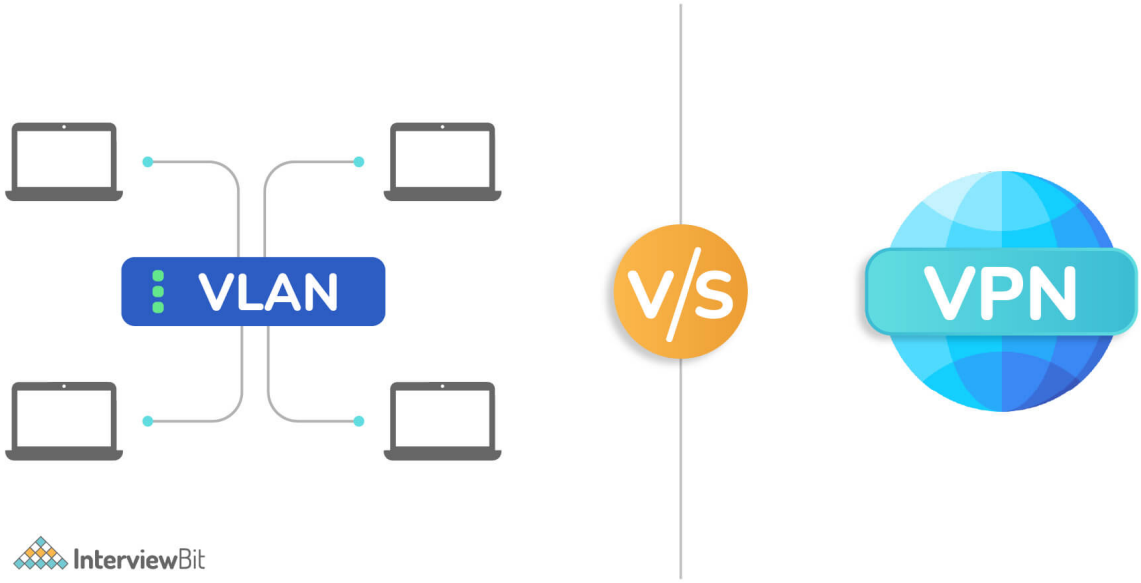
21. Differentiate between Information protection and information assurance.

Information protection protects data from unauthorized access by utilizing encryption, security software, and other methods.
Information Assurance ensures the data's integrity by maintaining its availability, authentication, and secrecy, among other things.

Cyber Security Interview Questions for Experienced

22. Differentiate between VPN and VLAN.

Companies use VLANs to consolidate devices that are dispersed across several remote sites into a single broadcast domain. VPNs, on the other hand, are used to transmit secure data between two offices of the same organization or between offices of different companies. Individuals also use it for their personal needs.
A VLAN is a VPN subtype. VPN stands for Virtual Private Network, and it is a technology that creates a virtual tunnel for secure data transfer over the Internet. Because it enables encryption and anonymization, a VPN is a more advanced but more expensive solution. A VLAN is useful for segmenting a network into logical sections for easier management, but it lacks the security characteristics of a VPN.
A virtual local area network minimizes the number of routers required as well as the cost of deploying routers. A VPN improves a network's overall efficiency.
Example of a VPN:- NordVPN, ZenMate



23. What do you mean by perimeter-based and data-based protection?

Perimeter-based cybersecurity entails putting security measures in place to safeguard your company's network from hackers. It examines people attempting to break into your network and prevents any suspicious intrusion attempts.

The term "**data-based protection**" refers to the use of security measures on the data itself. It is unaffected by network connectivity. As a result, you can keep track of and safeguard your data regardless of where it is stored, who accesses it, or which connection is used to access it.

24. Which is more reliable: SSL or HTTPS?

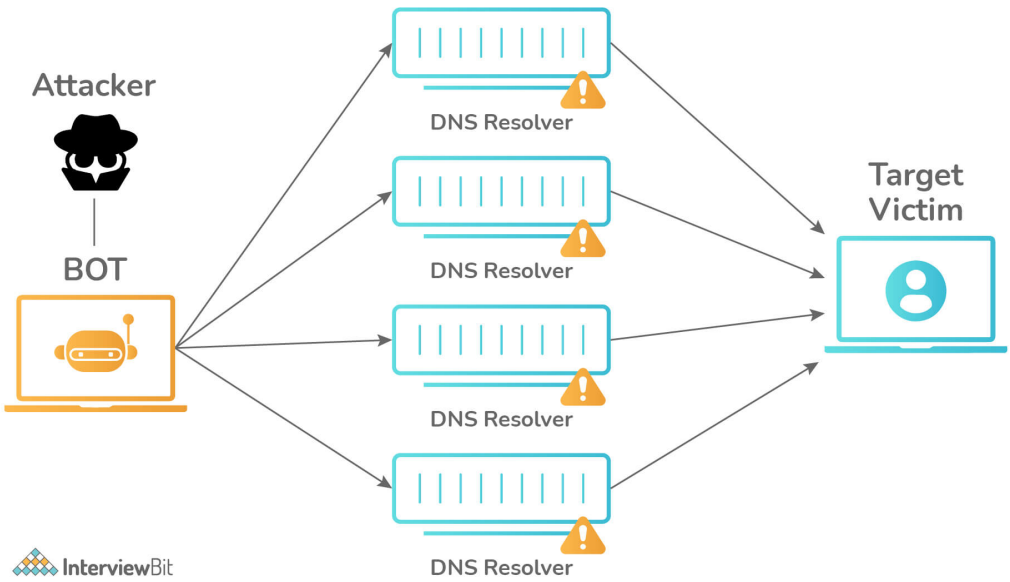
SSL (Secure Sockets Layer) is a secure technology that allows two or more parties to communicate securely over the internet. To provide security, it works on top of HTTP. It works at the Presentation layer.
HTTPS (Hypertext Transfer Protocol Secure) is a combination of HTTP and SSL that uses encryption to create a more secure surfing experience. The working of HTTPS involves the top 4 layers of the OSI model, i.e, Application Layer, Presentation Layer, Session Layer, and Transport Layer.
SSL is more secure than HTTPS in terms of security.

25. Differentiate between Symmetric and Asymmetric Encryption.

Symmetric Encryption	Asymmetric Encryption
Both encryption and decryption can be done using just one key.	It takes two keys to encrypt and decrypt data respectively.
In this technique, the encryption system is very fast.	In this technique, the encryption system is slow.
When a huge volume of data must be transferred, it is used.	When a small volume of data must be transferred, it is used.
When compared to asymmetric key encryption, symmetric key encryption uses fewer resources.	When compared to symmetric key encryption, asymmetric key encryption uses more resources.
The ciphertext is the same size as or smaller than the plain text.	The ciphertext is the same size as or greater than the plain text.
Eg :- AES, DES	Eg :- DSA and RSA

26. What do you mean by a DDoS attack? How can you prevent it?

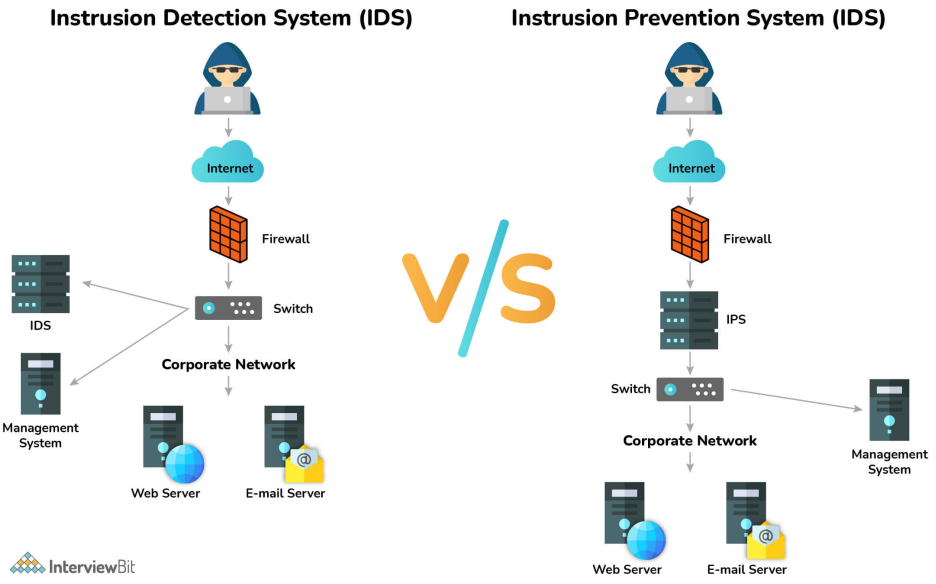
It's a form of cyber threat or malicious effort in which fraudsters use Internet traffic to fulfill legitimate requests to the target or its surrounding infrastructure, causing the target's regular traffic to be disrupted. The requests originate from a variety of IP addresses, which might cause the system to become unworkable, overload its servers, cause them to slow down or go offline, or prevent an organization from performing its essential responsibilities.



The methods listed below will assist you in stopping and preventing DDOS attacks:

- Create a denial of the service response strategy.
- Maintain the integrity of your network infrastructure.
- Use fundamental network security measures.
- Keep a solid network architecture.
- Recognize the Warning Signs
- Think about DDoS as a service.

27. Differentiate between IDS and IPS in the context of Cyber Security.



Intrusion Detection Systems (IDS) scan and monitor network traffic for signals that attackers are attempting to infiltrate or steal data from your network using a known cyber threat. IDS systems detect a variety of activities such as security policy violations, malware, and port scanners by comparing current network activity to a known threat database.

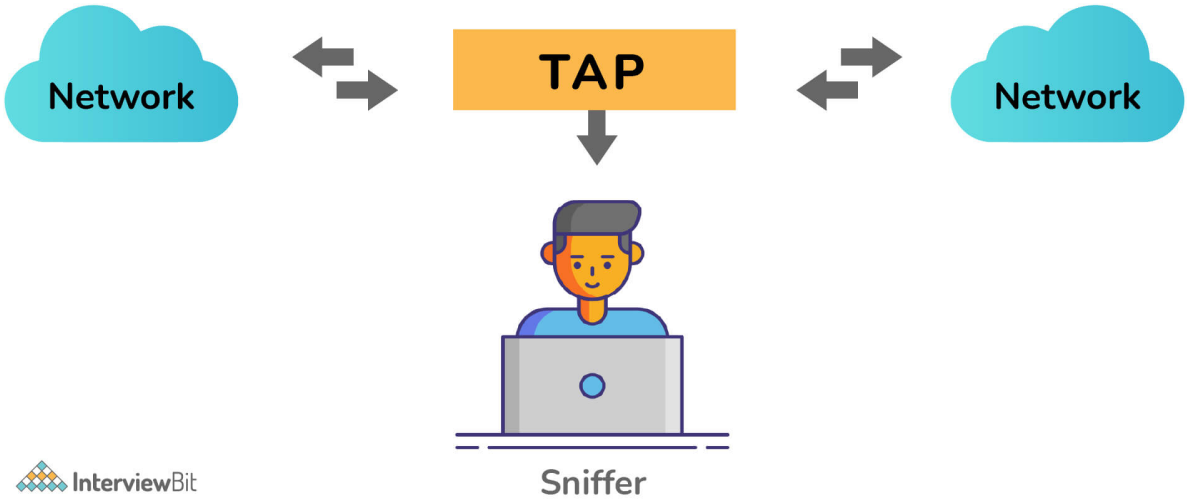
Intrusion Prevention Systems (IPS) are located between the outside world and the internal network, in the same area of the network as a firewall. If a packet represents a known security hazard, an IPS will proactively prohibit network traffic based on a security profile.

The fundamental distinction is that an IDS is a monitoring system, whereas an IPS is a control system. IDS makes no changes to network packets, whereas IPS block packet delivery depending on the contents of the packet, similar to how a firewall blocks traffic based on IP address.

28. What do you mean by Network Sniffing?

Sniffing is a technique for evaluating data packets delivered across a network. This can be accomplished through the use of specialized software or hardware. Sniffing can be used for a variety of purposes, including:

- Capture confidential information, such as a password.
- Listen in on chat messaging
- Over a network, keep an eye on a data package.



29. Differentiate between Black Box Testing and White Box Testing.

Black Box Testing	White Box Testing
It's a type of software testing in which the program's or software's internal structure is concealed.	It is a method of software testing in which the tester is familiar with the software's internal structure or code.
It is not necessary to have any prior experience with implementation.	It is not necessary to have prior experience with implementation.
On the basis of the requirement specifications paper, this testing can begin.	This form of software testing begins once the detailed design document has been completed.
It takes the least amount of time.	It takes the most amount of time.
It is the software's behavior testing.	It is the software's logic testing.
It is relevant to higher levels of software testing.	It is relevant to lower levels of software testing.

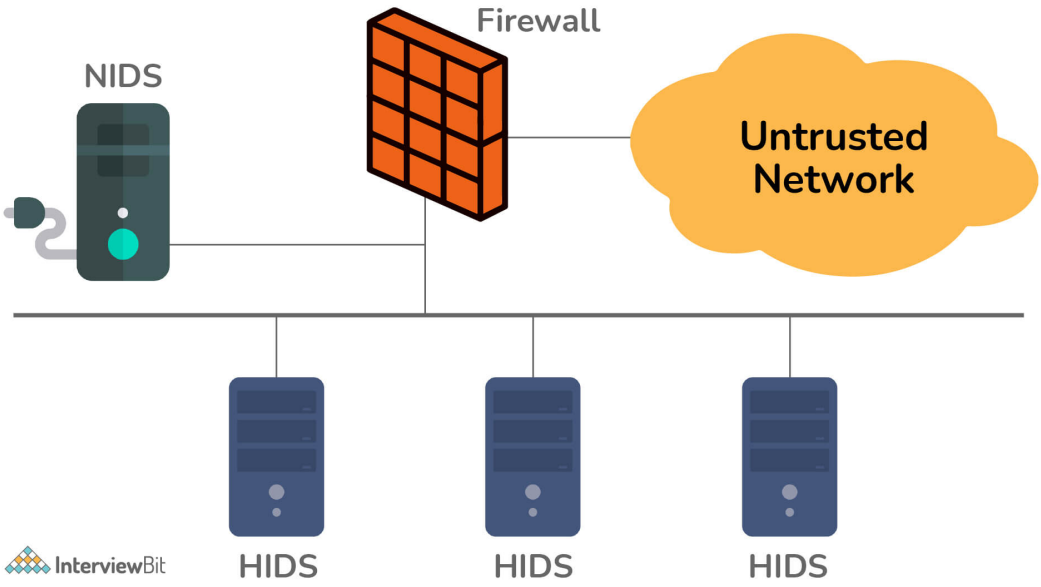
30. What do you mean by System Hardening?

In general, system hardening refers to a set of tools and procedures for managing vulnerabilities in an organization's systems, applications, firmware, and other components.
The goal of system hardening is to lower security risks by lowering potential attacks and compressing the system's attack surface.
The many types of system hardening are as follows:

- Hardening of databases
- Hardening of the operating system
- Hardening of the application
- Hardening the server
- Hardening the network

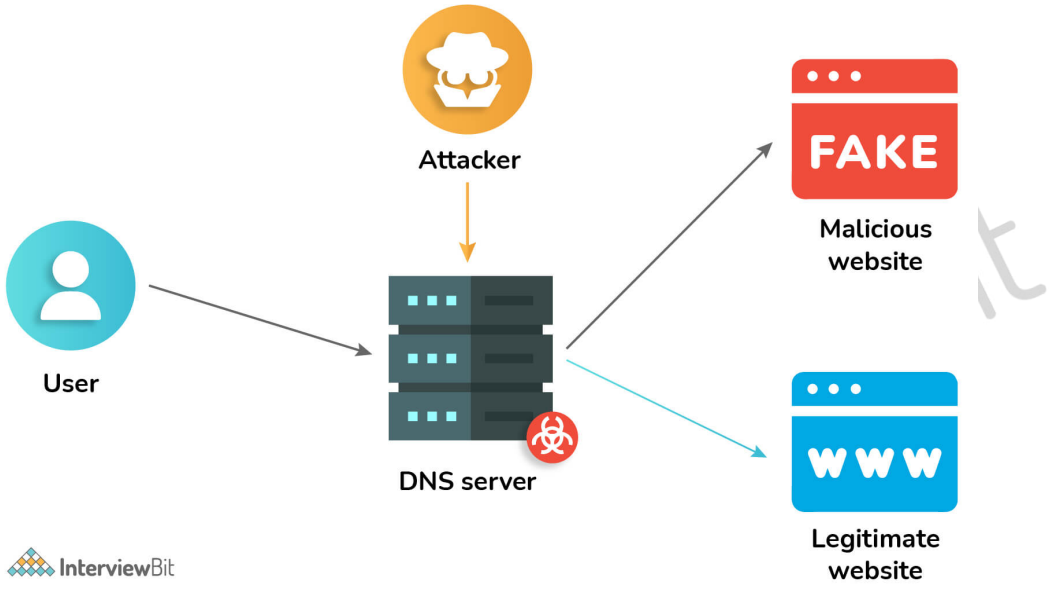
31. Differentiate between HIDS and NIDS.

HIDs look at certain host-based actions including what apps are run, what files are accessed, and what information is stored in the kernel logs. NIDs examine the flow of data between computers, often known as network traffic. They basically "sniff" the network for unusual activity. As a result, NIDs can identify a hacker before he can make an unlawful entry, whereas HIDs won't notice anything is wrong until the hacker has already gotten into the system.



32. What do you mean by Domain Name System (DNS) Attack?

DNS hijacking is a sort of cyberattack in which cyber thieves utilize weaknesses in the Domain Name System to redirect users to malicious websites and steal data from targeted machines. Because the DNS system is such an important part of the internet infrastructure, it poses a serious cybersecurity risk.



These can be avoided by the following precautions:-

- Examine the DNS zones in your system.
- Make sure your DNS servers are up to current.
- The BIND version is hidden.
- Transfers between zones should be limited.
- To avoid DNS poisoning attempts, disable DNS recursion.
- Use DNS servers that are separated.
- Make use of a DDOS mitigation service.

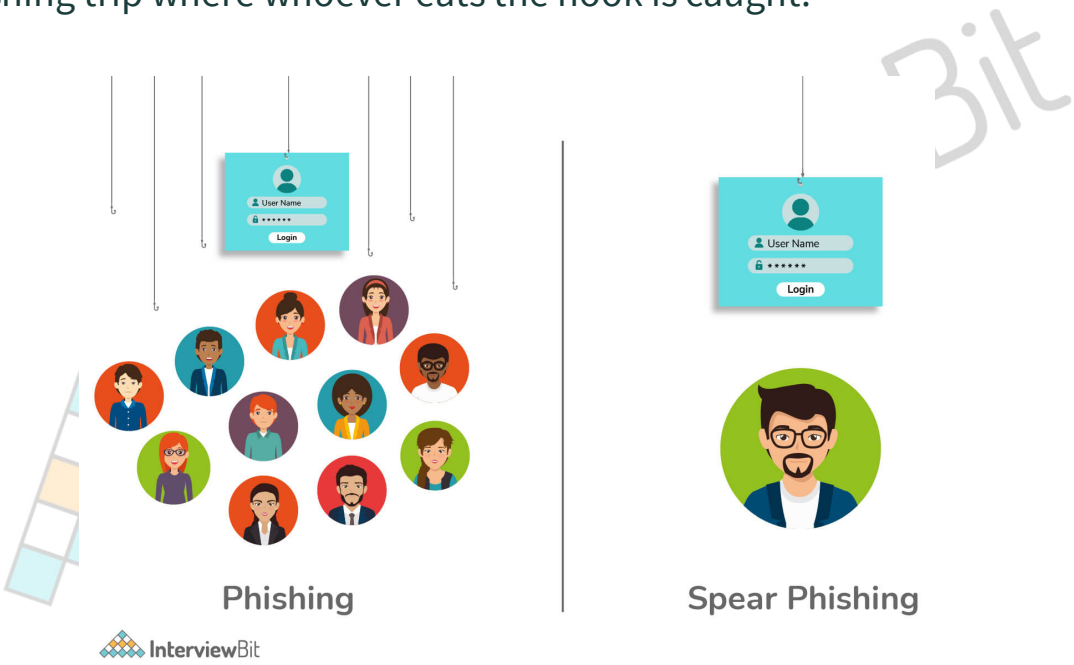
33. Differentiate between Stream Cipher and Block Cipher.

The major distinction between a block cypher and a stream cypher is that a block cypher turns plain text into ciphertext one block at a time. Stream cypher, on the other hand, converts plain text into ciphertext by taking one byte of plain text at a time.

Block Cipher	Stream Cipher
By converting plaintext into ciphertext one block at a time, Block Cipher converts plain text into ciphertext.	Stream Cipher takes one byte of plain text at a time and converts it to ciphertext.
Either 64 bits or more than 64 bits are used in block ciphers.	8 bits are used in stream ciphers.
The ECB (Electronic Code Book) and CBC (Common Block Cipher) algorithm modes are utilized in block cipher (Cipher Block Chaining).	CFB (Cipher Feedback) and OFB (Output Feedback) are the two algorithm types utilized in stream cipher (Output Feedback).
The Caesar cipher, polygram substitution cipher, and other transposition algorithms are used in the block cipher.	Stream cipher uses substitution techniques such as the rail-fence technique, columnar transposition technique, and others.
When compared to stream cipher, a block cipher is slower.	When compared to a block cipher, a stream cipher is slower.

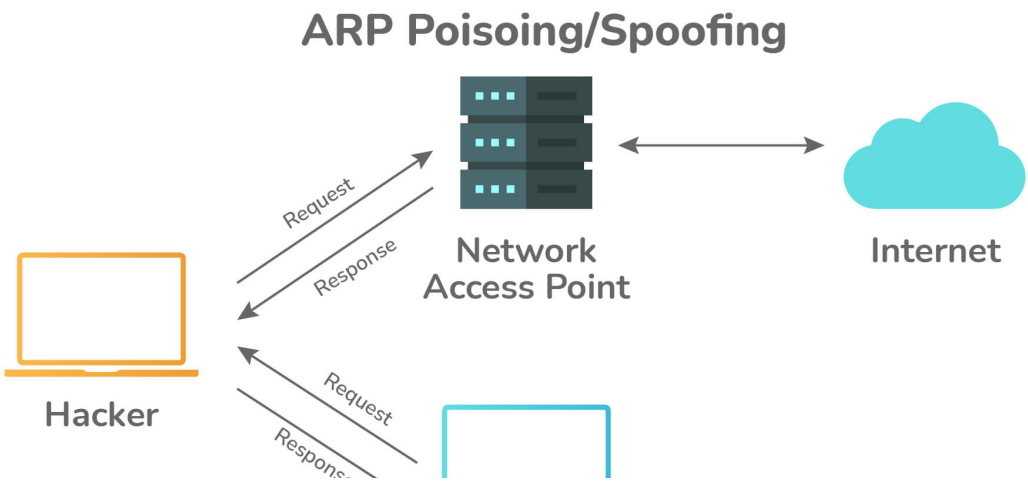
34. Differentiate between spear phishing and phishing?

Spear phishing is a type of phishing assault that targets a small number of high-value targets, usually just one. Phishing usually entails sending a bulk email or message to a big group of people. It implies that spear-phishing will be much more personalized and perhaps more well-researched (for the individual), whereas phishing will be more like a real fishing trip where whoever eats the hook is caught.



35. What do you mean by ARP poisoning?

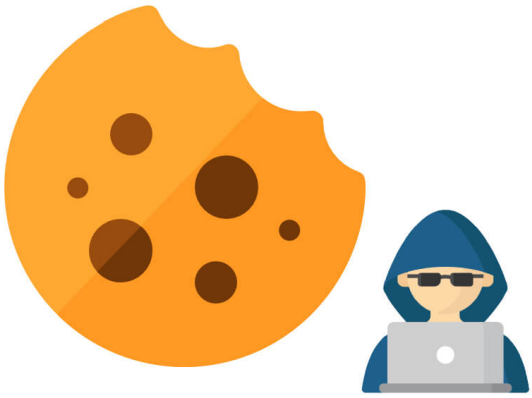
Address Resolution Protocol Poisoning is a sort of cyber-attack that uses a network device to convert IP addresses to physical addresses. On the network, the host sends an ARP broadcast, and the receiver machine responds with its physical address.
It is the practice of sending bogus addresses to a switch so that it can associate them with the IP address of a legitimate machine on the network and hijack traffic.



A virus is a piece of harmful executable code that is attached to another executable file and can modify or erase data. When a virus-infected computer application executes, it takes action such as removing a file from the computer system. Viruses can't be managed from afar.
Worms are comparable to viruses in that they do not alter the program. It continues to multiply itself, causing the computer system to slow down. Worms can be manipulated with remote control. Worms' primary goal is to consume system resources.

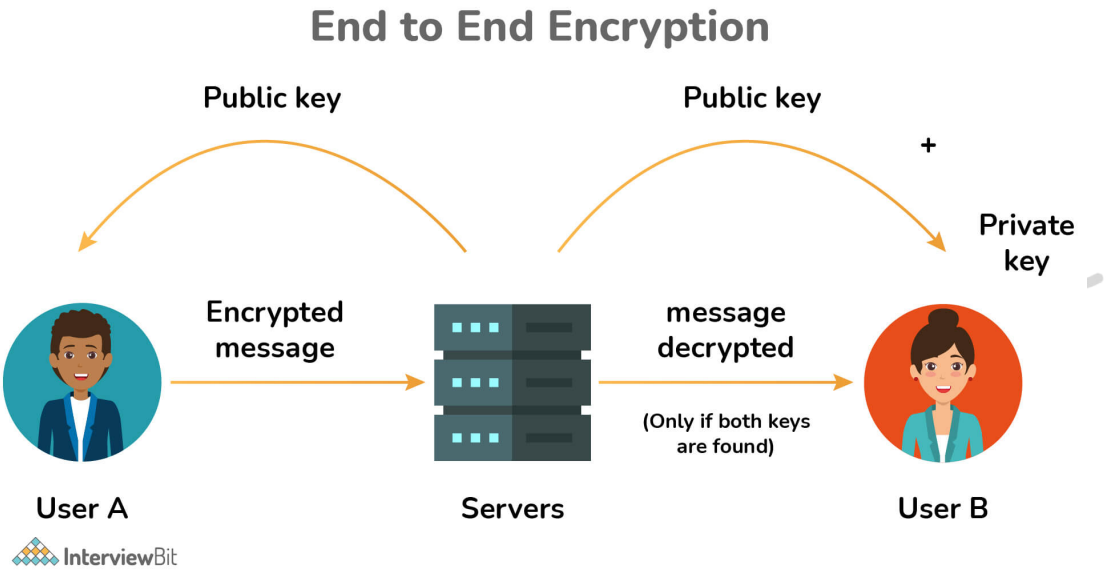
38. What form of cookie might be used in a spyware attack?

A tracking cookie, instead of a session cookie, would be used in a spyware attack because it would last through multiple sessions rather than just one.



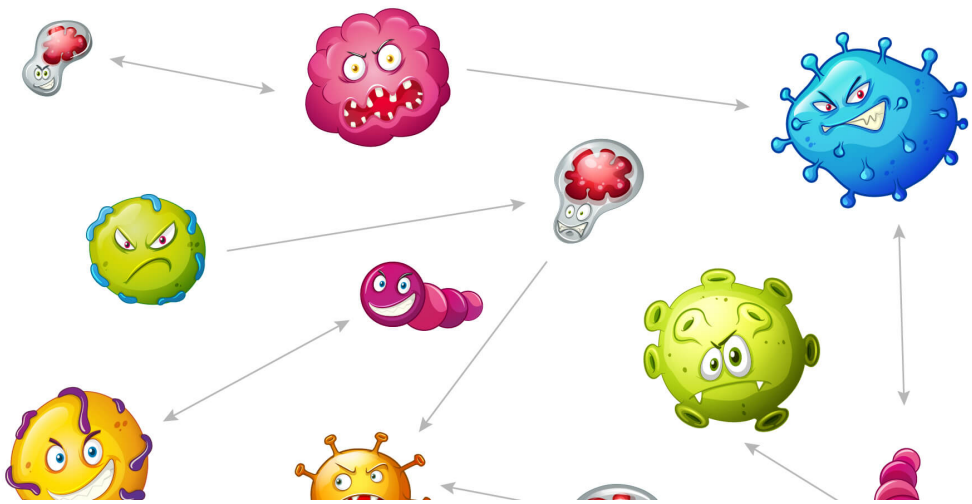
39. How do you decide the placement of the encryption function?

We must decide what to encrypt and where the encryption mechanism should be situated if encryption is to be used to counter attacks on confidentiality. Link and end-to-end encryption are the two main ways of encryption placement.
End-to-end encryption, or E2EE, is a secure data transfer system in which data is encrypted and decrypted only at the endpoints, regardless of how many points it passes through in the middle of its virtual journey. This sort of encryption is an excellent technique to communicate in a secure and confidential manner. Because



40. What are Polymorphic viruses?

Polymorphic viruses are sophisticated file infectors that may build changed versions of themselves in order to avoid detection while maintaining the same fundamental behaviors after each infection. Polymorphic viruses encrypt their programming and employ various encryption keys each time to alter their physical file makeup throughout each infection.
Mutation engines are used by polymorphic viruses to change their decryption routines every time they infect a machine. Because typical security solutions do not use a static, unchanging code, traditional security solutions may miss them. They are considerably more difficult to detect because they use complicated mutation engines that generate billions of decryption routines.



Forward secrecy is a property of certain key agreement protocols that ensures that the session keys will not be exposed if the server's private key is exposed. Perfect forward secrecy is another name for it (PFS).
The "Diffie–Hellman key exchange" algorithm is used to accomplish this.

Conclusion:

Cybersecurity is critical because it safeguards all types of data against theft and loss. Sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems all fall under this category.
Your company won't be able to defend itself if it doesn't have a cybersecurity program.
Cyber security awareness is defined as the knowledge of an action taken to secure a company's information assets. When employees at a company are cyber security conscious, it implies they understand what cyber dangers are, the possible impact a cyber-attack will have on their company, and the procedures necessary to reduce risk and prevent cyber-crime from penetrating their online workspace.
To learn more about Cyber Security, you can go through the following references:-

- Hacking: The Art of Exploitation by Jon Erickson
- Practical Malware Analysis by Michael Sikorski

Links to More Interview Questions

C Interview Questions	Php Interview Questions	C Sharp Interview Questions
Web Api Interview Questions	Hibernate Interview Questions	Node Js Interview Questions
Cpp Interview Questions	Oops Interview Questions	Devops Interview Questions
Machine Learning Interview Questions	Docker Interview Questions	Mysql Interview Questions
Css Interview Questions	Laravel Interview Questions	Asp Net Interview Questions
Django Interview Questions	Dot Net Interview Questions	Kubernetes Interview Questions
Operating System Interview Questions	React Native Interview Questions	Aws Interview Questions
Git Interview Questions	Java 8 Interview Questions	Mongodb Interview Questions
Dbms Interview Questions	Spring Boot Interview Questions	Power Bi Interview Questions
Pl Sql Interview Questions	Tableau Interview Questions	Linux Interview Questions
Ansible Interview Questions	Java Interview Questions	Jenkins Interview Questions