

## 1. What is cryptography?



**Cryptography aids to secure information from third parties who are called adversaries. It allows only the sender and the recipient to access the data securely.**

## 2. What is traceroute? Mention its uses.

```
prabhakar@inspiron-3542:~$ traceroute google.com
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets
 1 192.168.43.45 (192.168.43.45)  2.014 ms  2.313 ms  2.588 ms
 2 * * *
 3 10.45.1.230 (10.45.1.230)  75.449 ms  115.244 ms  115.224 ms
 4 10.45.8.178 (10.45.8.178)  93.056 ms  115.130 ms  93.022 ms
 5 10.45.8.187 (10.45.8.187)  115.116 ms  115.106 ms  115.070 ms
 6 * * *
 7 218.248.235.141 (218.248.235.141)  120.589 ms  108.033 ms  106.902 ms
 8 210.240.235.142 (210.240.235.142)  114.489 ms * *
 9 72.14.211.114 (72.14.211.114)  98.076 ms  93.232 ms  93.781 ms
10 108.170.253.113 (108.170.253.113)  98.688 ms  91.388 ms  108.170.253.97 (108.170.253.97)  107.241 ms
11 74.125.253.69 (74.125.253.69)  95.120 ms  72.14.237.105 (72.14.237.105)  102.594 ms  103.137 ms
12 naa03s23-ln-f14.1e100.net (172.217.26.206)  101.794 ms  97.907 ms  97.105 ms
prabhakar@inspiron-3542:~$
```

**Traceroute is a network diagnostic tool. It helps track the route taken by a packet that is sent across the IP network. It 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 where the point of failure is.**

### 3. What is a firewall? Mention its uses.



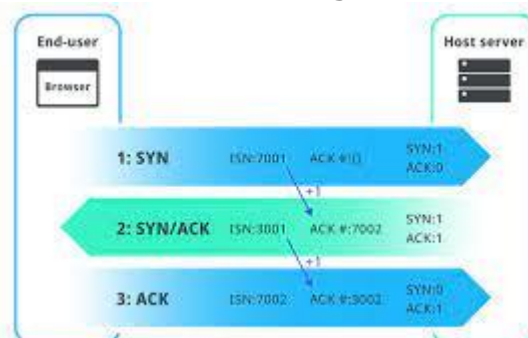
**A firewall is a network security device/system, which blocks malicious traffic such as hackers, worms, malware, and viruses to maintain data privacy.**

#### **Uses:**

**It monitors the incoming and outgoing network traffic. It permits or allows only data packets that agree to the set of security rules.**

**It acts as a barrier between the internal network and the incoming traffic from external sources like the Internet.**

### 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 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 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 Status Codes



**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 is continuing. 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:**

<https://www.ez-learn.global/>

**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. What are the common cyberattacks?



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

**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.**

**Phishing: Here, the attacker will act as a trusted entity to perform**

**malicious activities such as getting usernames, passwords, and credit card numbers.**

**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.**

**Malware:** Malware is software that is designed to attack the target system. The software can be a virus, worm, ransomware, spyware, and so on.

**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.

**DDoS:** This is done to overwhelm the target network with massive traffic, making it impossible for the website or the service to be operable.

**Malvertising:** Malvertising refers to the injections of maleficent code to legitimate advertising networks, which redirect users to unintended websites.

**Password Attacks:** As the name suggests, here, the cyber hacker cracks credentials like passwords.

## 8. What is data leakage?



**Data leakage means the unauthorized transmission of data from an organization to an external recipient. The mode of transmission can be electronic, physical, web, email, mobile data, and storage devices, such as USB keys, laptops, and optical media.**

### **Types of data leakage:**

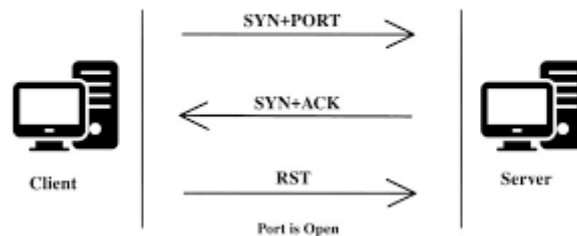
**Accidental leakage:** The authorized entity sends data to an unauthorized entity accidentally.

**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.

#### Port Scanning Attack

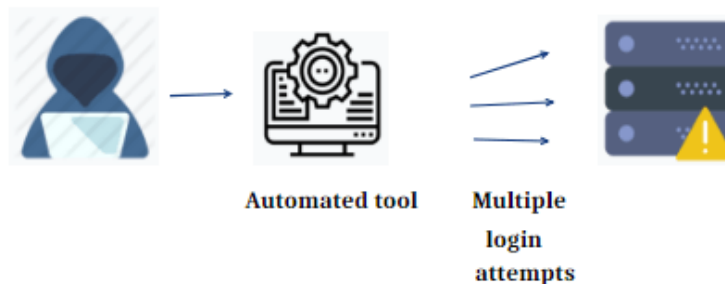


**A port scan helps you determine the ports that are open, listening, or closed on a network. Administrators use this to test network security and the system's firewall strength. For hackers, it is a popular reconnaissance tool to identify the weak point to break into a system.**

**Some of the common basic port scanning techniques are:**

**UDP**  
**Ping scan**  
**TCP connect**  
**TCP half-open**  
**Stealth scanning**

### 10. Explain brute force attack and the ways to prevent it.

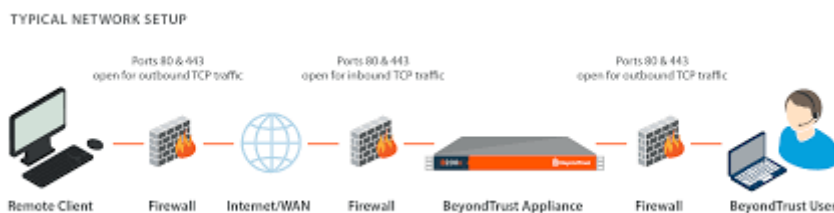


**A brute force attack is a hack where the attacker tries to guess the target password by trial and error. It is mostly implemented with the help of automated software used to login with credentials.**

**Here are some ways to prevent a brute force attack:**

- Set a lengthy password**
- Set a high-complexity password**
- Set a limit for login failures**

### **11. Mention the steps to set up a firewall.**



**Following are the steps you have to follow to set up a firewall:**

- Username/password: Alter the default password of a firewall device.**
- Remote Administration: Always disable the Remote Administration feature.**
- Port Forward: For the web server, FTP, and other applications to work properly, configure appropriate ports.**
- DHCP Server: Disable the DHCP server when you install a firewall to avoid conflicts.**
- Logging: Enable logs to view the firewall troubleshoots and to view logs.**



**Policies: Configure strong security policies with the firewall.**

## 12. What is SSL encryption?

### SSL Encryption (HTTPS)



**Secure Socket Layer is a security protocol that is used for the purpose of encryption. It ensures privacy, data integrity, and authentication in the network like online transactions.**

**The following are the steps for setting up an SSL encryption:**

**A browser connects to an SSL-secured web server.**

**The browser requests the server's public key in exchange for its own private key.**

**If it is trustworthy, the browser requests to establish an encrypted connection with the web server.**

**The web server sends the acknowledgement to start an SSL encrypted connection.**

**SSL communication starts to take place between the browser and the web server.**

## 13. What steps will you take to secure a server?

<https://www.ez-learn.global/>



**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**

#### **14. What are the different layers of the OSI model?**



**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.**

**Datalink 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.**

### 15. What is a VPN?



**VPN stands for virtual private network. It is a private network that gives you online anonymity and privacy from a public Internet connection. VPN helps you protect your online activities, such as sending an email, paying bills, or shopping online.**

#### **How does a VPN work?**

**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).**

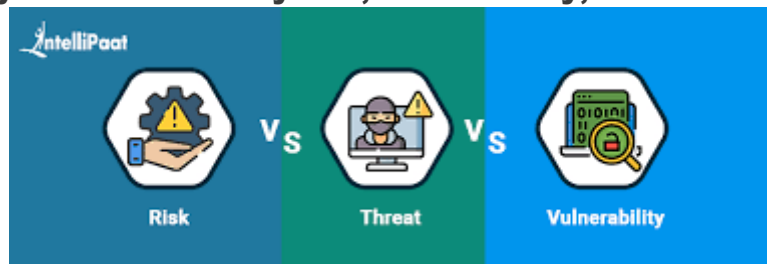
**During this transmission, your data is encrypted and sent through another point on the Internet.**

**When it reaches the server, the data is decrypted.**

**The response from the server reaches the VPN where it is encrypted, and it**

**will be decrypted by another point in the VPN.  
At last, the data, which is decrypted, reaches you.**

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



**Threat: A cyber security threat can cause potential harm to an organization's assets by exploiting a vulnerability. It can be intentional or accidental.**

**Vulnerability: A vulnerability is a weakness or a gap in the security system that can be taken advantage of by a malicious hacker.**

**Risk: A risk happens when the threat exploits a vulnerability. It results in loss, destruction, or damage to the asset.**

**17. How do you prevent identity theft?**



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

**Protect your personal records.**

**Avoid online sharing of confidential information.**

**Protect your Social Security Number.**

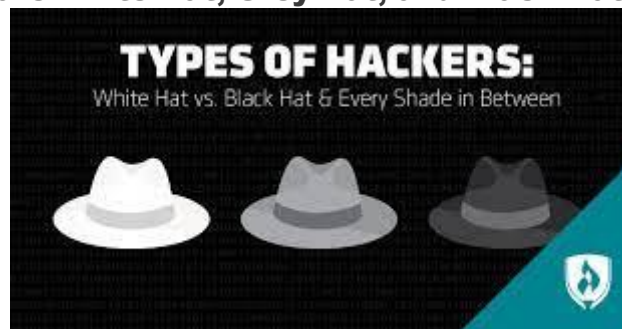
**Use strong passwords, and change them at regular intervals.**

**Do not provide your bank information on untrustworthy websites.**

**Protect your system with advanced firewall and spyware tools.**

**Keep your browsers, system, and software updated.**

**18. 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.**

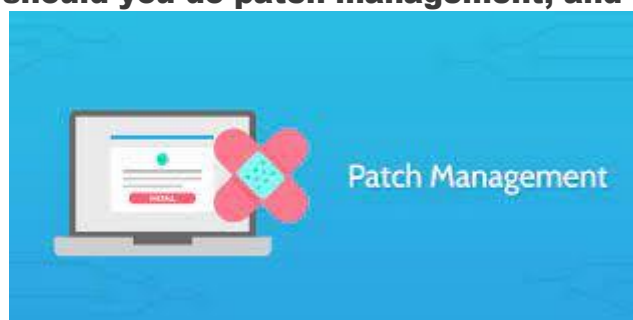
**White Hat Hackers**

**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.**

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



**Patch management has to be done immediately once the updates to the software is released. All the network devices in the organization should get patch management in less than a month.**

**20. 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:**

**you need to unplug the PC and remove the CMOS battery in the cabinet for 15–30 minutes. Then, you can put it back.**

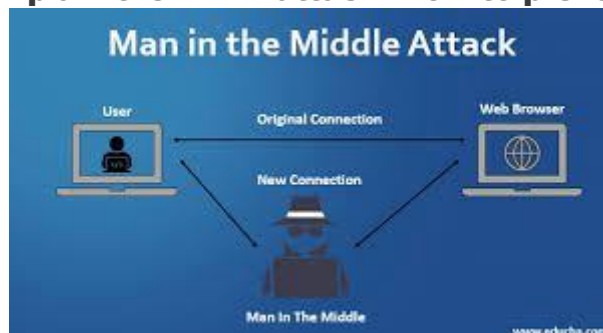
**You can use third-party software such as CmosPwd and Kiosk.**

**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 need to re-enter the settings for it.**

**21. 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:**

**Public key pair based authentication**

**Virtual private network**

**Strong router login credentials**

**Implement a well-built Intrusion Detection Systems (IDS) like firewalls.**

**Strong WEP/WPA encryption on access points**

## **22. 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. DDoS 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:**

- Configure firewalls and routers**
- Recognize the spike in traffic**
- Consider front-end hardware**
- Empower the server with scalability and load balancing**
- Use anti-DDoS software**

**23. Explain the XSS attack. How to prevent it?**



**Cross-site scripting also known as XSS attack allows the attacker to pretend as a victim 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 victim 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:**

- Cross-check user's input**
- Sanitize HTML**
- Employ anti-XSS tools**
- Use encoding**
- Check for regular updates of the software**

**24. 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:**

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

**All nodes on the network receive the ARP request.**

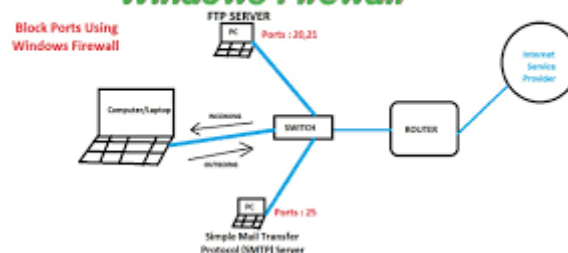
**The nodes check whether the request matches with the ARP table to find the target's MAC address.**

**If it does not match, then the nodes silently discard the packet.**

**If it matches, the target will send an ARP response back to the original sender via unicast.**

**25. What is port blocking within LAN?**

**Block Network Port's using Windows Firewall**



**It refers to restricting users from accessing a set of services within the local area network. The main aim is to stop the source from providing access to destination nodes via ports. Since all applications run on the**

**ports, it is necessary to block the ports to restrict unauthorized access, which might violate the security vulnerability in the network infrastructure.**

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

TCP/IP Model	Layer	Protocols
EduKedar	Application	HTTP,FTP,POP3, SMTP,SNMP
	Transport	TCP,UDP
	Networking	IP,ICMP
	Datalink	Ethernet, ARP

**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**

**27. What is a botnet?**

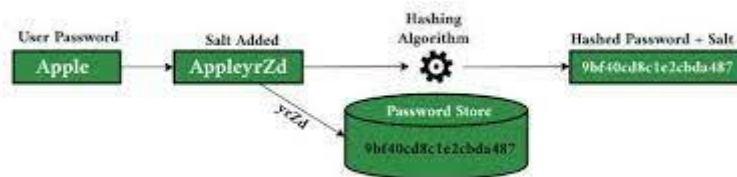


**A botnet, which is also known as a robot network, is a malware that infects networks of computers and gets them under the control of a single attacker who is called a 'bot herder.' A bot is an individual machine that is under the control of bot herders. The attacker acts as a central party who can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

**The botnet is a large-scale attack since a bot herder can control millions of**

**bots at a time. All the botnets can receive updates from the attacker to change their behavior in no time.**

### 28. 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.**

### 29. Explain SSL and TLS.



## SSL/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 version protocol that works just like SSL to protect the information transfer. However, to provide better security, both TLS and SSL are often implemented together.**

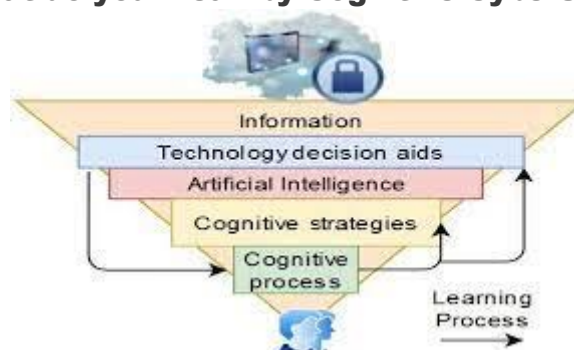
### **30. What is 2FA, and how can it be implemented for public websites?**



**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, he/she is prompted for 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.**

### **31. 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.**

**32. Explain phishing. How to 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:**

**Install firewalls**

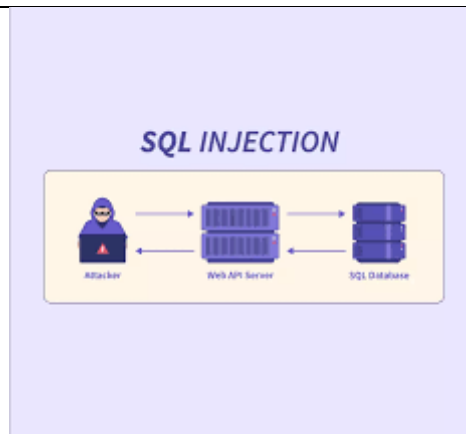
**Rotate passwords frequently**

**Do not click on or download from unknown sources**

**Get free anti-phishing tools**

**Do not provide your personal information on an unsecured/unknown site**

**33. 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 data integrity loss of an organization.**

**Ways to prevent SQL injection:**

- Limit providing read access to the database**
- Sanitize data with the limitation of special characters**
- Validate user inputs**
- Use prepared statements**
- Check for active updates and patches**

**34. 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.**

**Do not download the attachment as it may have malicious viruses, malware, or bugs, which might corrupt your system.**

**Do not visit any links as it might redirect you to an unintended page.**

**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.**

**Many websites masquerade as a legitimate site to steal sensitive information, so you should be careful not to fall into the wrong hands.**

<https://www.ez-learn.global/>

**35. 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.**

**36. To print billing, you have to provide your login credentials in your computing labs. Recently, people started to get a bill for the print, which was never done by them. When they called to complain, the bill turned out to be correct. How do you explain the above 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.**

**37. In our campus computer lab, one of my friends logged into her Yahoo account. When she left the lab, she made sure that the account was not left open. Later, she came to realize that someone re-accessed her account from the browser, which she has used to send emails, by impersonating her. How do you think this happened?**

**There are two possible scenarios:**

**The attacker can visit the browser's history to access her account if she hasn't logged out.**

**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)**

**38. An employee's bank account faces an error during a direct deposit. 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 confirmations that the error no longer exists. 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.**

**39. 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?**

**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.**

**40. Check out the list of passwords below, which are pulled out from a database:**

- 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:**

**Minimum of 8 characters in length**

**Having any of the three from these four types of characters: lower case, upper case, numbers, and special characters.**

**41. 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.**

**42. 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:**

**Dated antivirus software or the lack of it  
Dated updates or security patches  
That's all for now!**

**This blog has listed answers to the most frequently asked Cyber Security 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.**