# Entry Level Cybersecurity Interview Questions

***By Surendra Pander {@technical surendra}***

## Cyber Security Interview Questions - Cyberattacks

This section of cyber security interview questions is based on cyberattacks.

### 65. What is SQL injection?

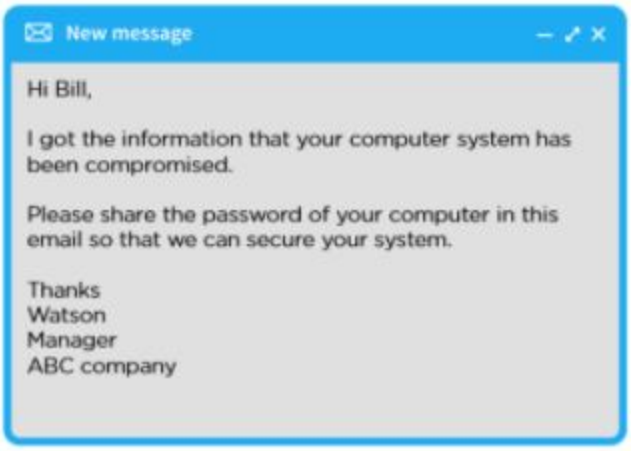
An SQL injection vulnerability enables an attacker to inject malicious input into an SQL statement. This attack allows the attackers to view, edit, and delete tables in a database. Additionally, attackers can also obtain administrative rights.

The types of SQL injection are:

1. In-band SQLi: Error-based and Union-based
2. Blind SQLi: Boolean-based and Time-based
3. Out-of-bound SQLi

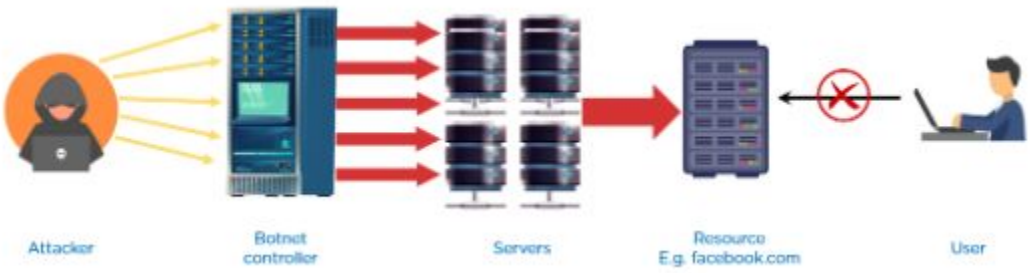
### 66. What is Spoofing?

In spoofing, an attacker pretends to be another person or organization and sends you an email that appears to be legitimate. The email looks almost genuine, and it is hard to spot such a fake one. An example of such an email is as follows:




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

A Denial of Service attacks' objective is to flood networks and systems with traffic to exhaust their resources and bandwidth. By doing so, a website is unable to cater to legitimate service requests. When hackers use multiple systems to launch this attack, it is known as a Distributed Denial of Service (DDOS) attack.




## 68. How to avoid ARP poisoning?

The following steps can avoid ARP poisoning:

1. Using Packet Filtering: Packet filters filter out and block packets that have the same source address data.
2. Keeping away from trust relationships: Organizations develop protocols that do not depend on trust relationships.
3. Utilize ARP Spoofing Software: ARP spoofing software gauges the information before transmission and blocks the information that is spoofed.

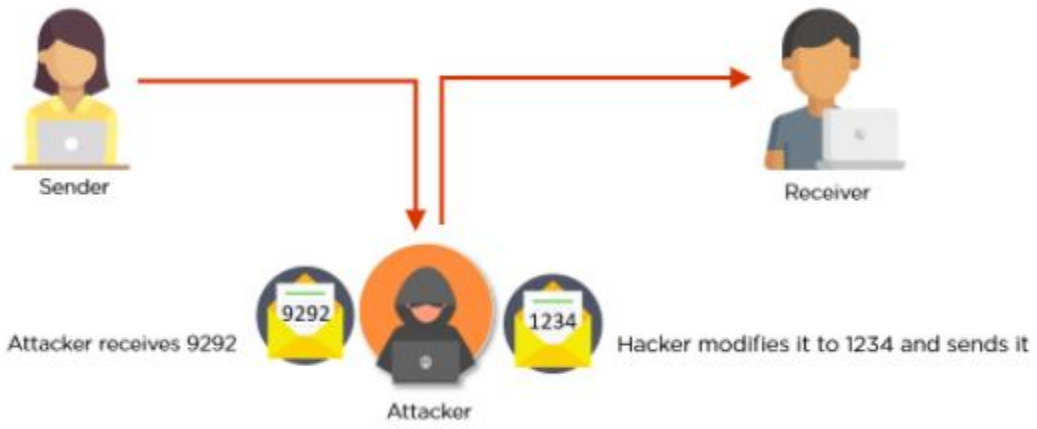
## 69. What is ransomware?

Ransomware blocks victims from accessing personal files and demands a ransom to regain access. It is a type of malware. There are three categories of ransomware:

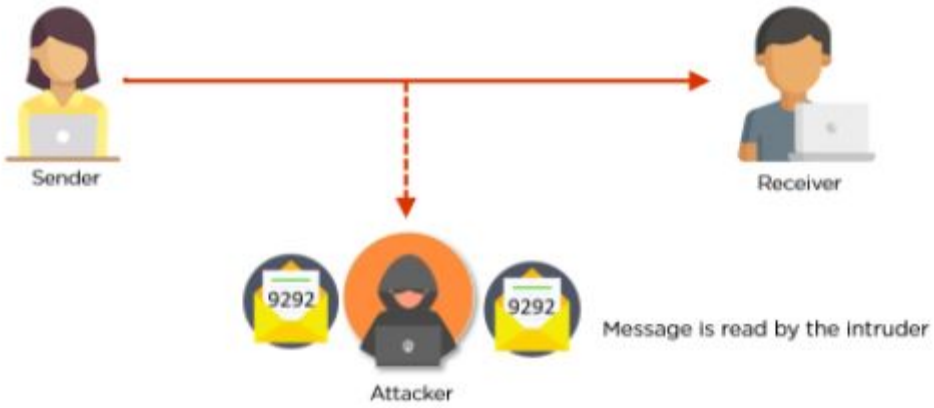
1. Scareware: It is a form of malware that uses social engineering to cause fear or anxiety to manipulate users into buying unwanted software.
2. Screen Lockers: Here, the users' computers are locked, and it displays an official-looking message. It thus prevents them from logging in to their computers.
3. Encrypting Ransomware: The ransomware displays a message demanding payment in return for the private asymmetric key needed to decrypt the encrypted file's symmetric keys.

## 70. What is the difference between active and passive cyberattacks?

As seen below, in an active attack, the attacker attempts to disrupt a network's normalcy, edits data, and alters the system resources.




Whereas, in a passive attack, the hacker intercepts the data traveling through the network. Here as seen below, the intruder eavesdrops but does not modify the message.




## 71. What is a social engineering attack?

Social engineering attacks manipulate people so that they end up sharing their confidential information. This attack has three categories:

1. Phishing Attack: Here, the user opens the mail with the attachment and unknowingly downloads the virus.
2. Spear Phishing Attack: Here, the attacker targets a specific individual or a group of people.
3. Whaling Phishing Attack: Whaling Phishing attack is a type of attack that specifically targets wealthy, powerful, and prominent individuals.

## 72. What is the man in the middle attack?

Here, the attacking computer takes the IP address of the client. The server continues communicating with the attacker, unaware of this.

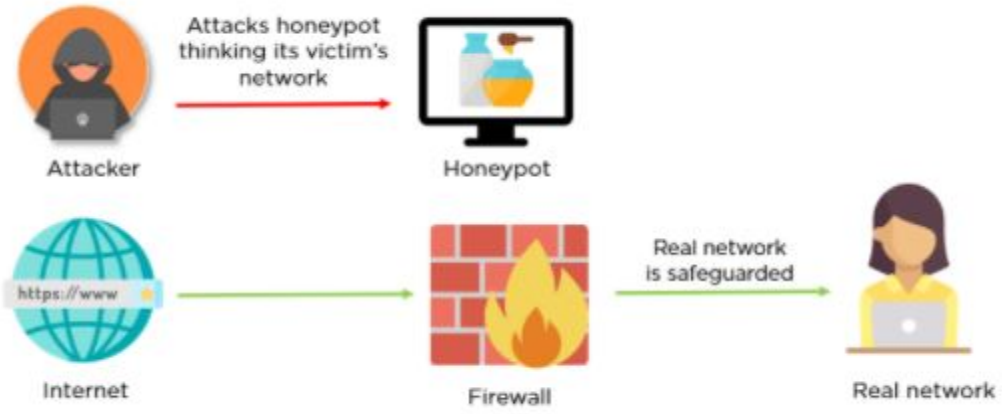
## 73. Who are black hat hackers and white hat hackers?

Black hat hackers are highly skilled individuals who illegally hack into a system. The motive behind this is mostly for monetary gain. These individuals are also known as security crackers.

White Hat Hackers, also called ethical hackers, are individuals who discover vulnerabilities in a computer network. Such a hacker works to defend organizations and governments.

## 74. What are honeypots?

Honeypots are computer systems that are used to lure attackers. It is used to deceive attackers and defend the real network from any attack. As seen below, the real network is safeguarded.




Let's now head to the final section of this article on cybersecurity interview questions.

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

https://www.buymeacoffee.com/surendrapander

**My social medial accounts -**

**Twitter — https://twitter.com/technicalSure**

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

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

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