1 What are the Different types of hackers-

1) Black Hat Hacker

- Black hat hackers are the evil guys who want to use their technical skills to defraud and blackmail others.
- They usually have the expertise and knowledge to break into computer networks without the owners' permission, exploit security vulnerabilities, and bypass security protocols.

2) White Hat Hacker

- White hat hackers (also known as ethical hackers) are the polar opposite of their black hat counterparts.
- They use their technical skills to protect the world from bad hackers.
- White hat hackers employ the same hacking techniques as black hat hackers, but they do it with the system owner's permission and their intentions are noble.

3) Grey Hat Hacker

- These hackers fall somewhere between white hat and black hat hackers.
- Grey hat hackers' intentions are often good, but they don't always take the ethical route with their hacking technics.
- For example, they may penetrate your website, application, or IT systems to look for vulnerabilities without your consent. But they typically don't try to cause any harm.

4) Red Hat Hacker

- Much like white hat hackers, red hat hackers also want to save the world from evil hackers.
- But they choose extreme and sometimes illegal routes to achieve their goals. Red hat hackers are like the pseudo-Robin Hood of the cybersecurity field — they take the wrong path to do the right thing.
- When they find a black hat hacker, they deploy dangerous cyber-attacks against them.

5) Blue Hat Hacker

- These hackers don't necessarily care about money or fame. They hack to take personal revenge for a real — or perceived — sleight from a person, employer, institution, or government.
- Blue hat hackers use malware and deploy various cyber-attacks on their enemies' servers/networks to cause harm to their data, websites, or devices.

6) Green Hat Hacker

- These are the "newbies" in the world of hacking. Green hat hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community.
- Although their intention is not necessarily to cause harm, they may do so while "playing" with various malware and attack techniques.

2. What are the different types of attacks?

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Web-based attacks-

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks-

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

3 Interfaces in Java

- An interface in Java is a blueprint of a class. It has static constants and abstract methods.
- The interface in Java is a mechanism to achieve abstraction.
- There can be only abstract methods in the Java interface, not method body.
- It is used to achieve abstraction and multiple inheritance in Java.
- In other words, interfaces can have abstract methods and variables. It cannot have a method body.
- Java Interface also represents the IS-A relationship.
- An interface is declared by using the interface keyword.
- It provides total abstraction; means all the methods in an interface are declared with the empty body, and all the fields are public, static and final by default.
- A class that implements an interface must implement all the methods declared in the interface.

Syntax:

```
1. interface <interface_name>{
2.
3.     // declare constant fields
4.     // declare methods that abstract
5.     // by default.
6. }
```

4 lambda in java-

- Lambda expression is a new and important feature of Java which was included in Java SE 8.
- It provides a clear and concise way to represent one method interface using an expression.
- It is very useful in collection library.
- It helps to iterate, filter and extract data from collection.

5 #pragma in c-

This directive is a special purpose directive and is used to turn on or off some features. This type of directives are compiler-specific i.e., they vary from compiler to compiler. Some of the #pragma directives are discussed below:

1. **#pragma startup and #pragma exit**: These directives helps us to specify the functions that are needed to run before program startup(before the control passes to main()) and just before program exit (just before the control returns from main()).
2. **#pragma warn Directive**: This directive is used to hide the warning messages which are displayed during compilation. This may be useful for us when we have a large program and we want to solve all the errors before looking on warnings then by using it we can focus on errors by hiding all warnings.
3. **#pragma GCC poison**: This directive is supported by the GCC compiler and is used to remove an identifier completely from the program. If we want to block an identifier then we can use the **#pragma GCC poison** directive.
4. **#pragma GCC dependency**: The #pragma GCC dependency allows you to check the relative dates of the current file and another file.
5. **#pragma GCC system_header**: This pragma takes no arguments. It causes the rest of the code in the current file to be treated as if it came from a system header.
6. **#pragma once**: The #pragma once directive has a very simple concept. The header file containing this directive is included only once even if the programmer includes it multiple times during a compilation.