**1. Different types of hackers**

* White hat hackers
* Black hat hackers
* Gray hat hackers
* Green hat hackers
* Script kiddies
* Red hat hackers
* Blue hat hackers

**White hat hackers:**

* These type of hackers are expertise in cybersecurity.
* They are authorized or certified to hack the system.
* They work for governments or organizations by getting into the system.
* They hack the system from the loopholes in the cybersecurity of the organization.
* They avoid attacks from external source

**Black hat hackers:**

* They attack other systems to get access to system where they do not have authorized entry.
* On gaining entry they might steal the data or destroy the system.
* Hacking practices used by these hackers depend on individuals hacking capacity and knowledge.

**Gray hat hackers:**

* These type of hackers falls in between black hat hackers and white hat hackers.
* They are not certified hackers.
* These type of hackers work with either good or bad intentions.
* The intention behind the hacking decides the type of hacker.
* If the intention if for personal gain then hacker is considered to be a gray hat hacker.

**Green hat hackers:**

* Theintention is to strive and learn to become full-fledged hacker.
* They will look for opportunity to learn from experienced hackers**.**

**SCRIPT KIDDIES:**

* They are amateur type of hackers .They try to hack the system with scripts from other fellow hackers.
* They try to hack the system networks ,websites etc
* The intention is just to get attention from their peers.

**Blue hat hackers:**

* They use hacking as a weapon to gain popularity among their fellow beings.
* Are dangerous due to the intent behind the hacking rather than knowledge

**Red hat hackers:**

* Similar to white hackers Intention is to stop the attack of black hat hackers.
* Red hat hackers are quite ruthless while dealing with black hat hackers.

**2.Different kinds of attacks**

* Phishing
* Man-in-the-middle attack
* Denial-of-service attack
* Spear phishing attack
* Ransomware attack
* Password attack
* Sql injection attack
* Brute force attack
* Web attacks
* Birthday attack
* Drive by attack

**Phishing attack:**

* occurs when a malicious actor sends emails that seem to be coming from trusted sources in an attempt to grab sensitive information from the target.

**Man-in-the-middle attack:**

* attackers refer to breaches in cybersecurity that makes it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks or computers.
* It is called man in middle attack because the attacker positions themselves in the middle or between the two parties trying to communicate.

**Denial of service attack and distributed Dos:**

* A denial-of-service attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests.
* distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system.
* DoS and DDoS attacks are different from other types of attacks that enable the hacker to either obtain access to a system or increase the access they currently have.
* With these types of attacks, the attacker directly benefits from their efforts.
* With DoS and DDoS attacks, on the other hand, the objective is simply to interrupt the effectiveness of the target's service.

**Spear phishing attack:**

* refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant.
* These types of attacks are called “spear” phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

**Ransomware attack:**

* In a ransomware attack, the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system’s manufacturer or the IT team.
* The ransomware then encrypts the target's workstation. At times, ransomware can be used to attack multiple parties by denying access to either several computers or a central server essential to business operations.

**Password Attack:**

* A hacker can also use a dictionary attack to ascertain a user’s password. A dictionary attack is a technique that uses common words and phrases, such as those listed in a dictionary, to try and guess the target's password.
* people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them.

**Sql injection attack:**

* Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users.
* Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server.
* The command is inserted, or “injected”, into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

**Brute Force attack:**

* The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in.
* These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account

**Web attacks:**

* Web attacks refer to threats that target vulnerabilities in web-based applications. Every time you enter information into a web application, you are initiating a command that generates a response.
* For example, if you are sending money to someone using an online banking application, the data you enter instructs the application to go into your account, take money out, and send it to someone else’s account. Attackers work within the frameworks of these kinds of requests and use them to their advantage.

**Birthday attack:**

* an attacker abuses a security feature hash algorithm, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic.
* If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender’s message with their own. The receiving device will accept it because it has the right hash.

**Drive by attack:**

* a hacker embeds malicious code into an insecure website. When a user visits the site, the script is automatically executed on their computer, infecting it.
* The designation “drive by” comes from the fact that the victim only has to “drive by” the site by visiting it to get infected. There is no need to click on anything on the site or enter any information.

**3. Interface 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 java interface, not method body. It is used to achieve abstraction and multiple inheritance in java.
* In simple words, an interface can have abstract methods and variables it cannot have method body.
* An interface is declared using the interface keyword. It provides all the methods in an interface are declared with the empty body and all the fields are public, static and final by default.

**4. Use of lambda expression in java**

* The lambda expression is used to provide the implementation of an interface which has functional interface.
* It saves a lot of code.
* In lambda expression, we do not need to define the method again for implementation just write the implementation code.
* Lambda expression provides implementation of functional interface.

5. #pragma Directive in C

* The #pragma directive is the method specified by the C standard for providing additional information to the compiler.
* The #pragma directive is used by the compiler to offer machine or operating system feature.
* This type of directive are compiler specific. They vary from compiler to compiler.

Syntax:

#pragma token

**6. Collections in JAVA?**

* The java collection is a framework that provides an architecture to store and manipulate the group of objects.
* Java collections can achieve all the operations that we perform on a data such as searching, sorting, insertion, manipulation and deletion.
* Java collection means a single unit of objects.