**What are the different types of attacks?**

Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine. Phishing is an increasingly common cyberthreat.

### Man-in-the-middle attack

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor’s device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim’s information.

### Denial-of-service attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a [distributed-denial-of-service (DDoS) attack](https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html).

### SQL injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

**What are different types of hackers?**

**White Hat Hackers**

White hat hackers are types of hackers who’re professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work as per the rules and regulations set by the government.  White hat hackers are also known as ethical hackers.

### **Black Hat Hackers**

Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used by these types of hackers depend on the individual’s hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.

### **Gray Hat Hackers**

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

### **Green Hat Hackers**

Green hat hackers are types of hackers who’re learning the ropes of hacking. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

### **Blue Hat Hackers**

The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

### **Red Hat Hackers**

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who’re similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is in the process of hacking through intention remains the same. Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

**What are interfaces in Java?**

The interface in Java is a mechanism to achieve [abstraction](https://www.javatpoint.com/abstract-class-in-java)*.* There can be only abstract methods in the Java interface, not method body. It is used to achieve abstraction and multiple [inheritance in Java](https://www.javatpoint.com/inheritance-in-java).

Example:

interface printable{

void print();

}

class A6 implements printable {

public void print()

{

System.out.println("Hello");

}

public static void main(String args[]){

A6 obj = new A6();

obj.print();

 }

}

**What is lambda function 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 case of lambda expression, we don't need to define the method again for providing the implementation. Here, we just write the implementation code.

**interface** Sayable{

**public** String say();

}

**public** **class** LambdaExpressionExample{

**public** **static** **void** main(String[] args) {

    Sayable s=()->{

**return** "I have nothing to say.";

    };

    System.out.println(s.say());

}

}

**What is #pragma in C?**

The #pragma pre-processor directive is used to provide additional information to the compiler. The #pragma directive is used by the compiler to offer machine or operating-system feature.

Some of the #pragma directives supported in Turbo C

#pragma argsused

#pragma exit

#pragma hdrfile

#pragma hdrstop

#pragma inline

#pragma option

#pragma saveregs

#pragma startup

#pragma warn