ASSIGNMENT-1

**1.Types of Hackers**

1. [White Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#White-Hat-Hackers)
2. [Black Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Black-Hat-Hackers)
3. [Gray Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Gray-Hat-Hackers)
4. [Script Kiddies](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Script-Kiddies)
5. [Green Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Green-Hat-Hackers)
6. [Blue Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Blue-Hat-Hackers)
7. [Red Hat Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Red-Hat-Hackers)
8. [State/Nation Sponsored Hackers](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#State/Nation-Sponsored-Hackers)
9. [Hacktivist](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Hacktivist)
10. [Malicious insider or Whistleblower](https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#Malicious-insider-or-Whistleblower).

### ****1) 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.

### 2) ****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

### 3) ****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.

### 4) ****Script Kiddies****

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs types of hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

### 5) ****Green Hat Hackers****

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

### 6) ****Blue Hat Hackers****

Blue Hat Hackers are types of hackers who’re similar to Script Kiddies. 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.

### 7) ****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.

### 8) ****State/Nation Sponsored Hackers****

Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids to be on top of every situation but also to avoid upcoming danger. They report only to their governments.

### 9) ****Hacktivist****

These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

### 10) ****Malicious insider or Whistleblower****

These types of hackers include individuals working in an organization who can expose confidential information. The intent behind the exposure might be a personal grudge with the organization or the individual might have come across the illegal activities within the organization. The reason for expose defines the intent behind the exposure. These individuals are known as whistleblowers.

**2.Different Types of attacks**

## Web-based attacks

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

**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.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*](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).

🡪In other words, you can say that interfaces can have abstract methods and variables. It cannot have a method body.

🡪Java Interface also **represents the IS-A relationship**

**4.Uses of Lambda expression:**

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.

Java lambda expression is treated as a function, so compiler does not create .class file.

1. To provide the implementation of Functional interface.
2. Less coding.

**5.#Pragma**

🡪The #pragma preprocessor 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.

Syntax: #pragma token

-->Different compilers can provide different usage of #pragma directive.