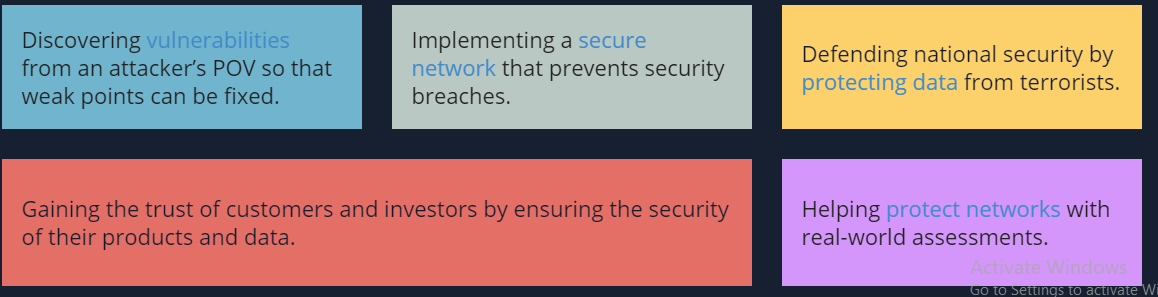
**Ethical Hacking**

**What is Ethical Hacking?**

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/ penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages.  The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

**Benefits of Ethical Hacking**



**Types of Ethical hacking:**



# Ethical Hacking - Hacker Types

## White Hat Hackers

White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

## Black Hat Hackers

Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

## Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.



## Miscellaneous Hackers

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it −

### Red Hat Hackers

### Blue Hat Hackers

### Elite Hackers

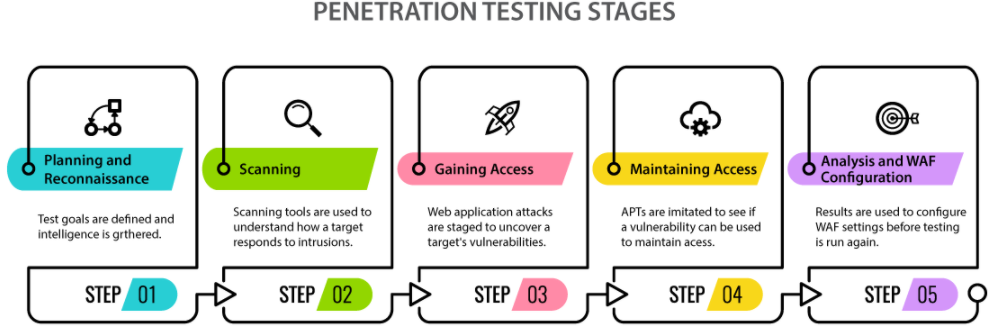
### Script Kiddie

### Neophyte

### Hacktivist

.

**Phases of Ethical Hacking**



### Planning and Reconnaissance:

The first step in ethical hacking is to define the scope and goals of a test as well as the testing methods to be followed. It also addresses intelligence to understand the potential vulnerabilities and how a target works. The prospective footprinting is made through search engines, web services, social network sites, DNS, email, network, etc. by using footprinting tools.

### Scanning:

In the second step, scanning is performed to understand how a target reacts to various intrusion attempts, in two ways – when the application’s code is static and when the application’s code is functioning. The later is the most practical way to understand the application’s performance in real-time.

### Gaining Access:

This is a crucial step where the web application is attacked using SQL injections, cross-site scripting, backdoors, etc. to find the vulnerabilities and then exploit them by stealing, intercepting traffic, and interfering privileges to understand the amount of damage that it can cause.

### Maintaining Access:

In this step of penetration testing, the vulnerability is used as a persistent presence for a long duration in the infected system in order to steal sensitive information or to spread inside the network, quickly gaining access to the server.

### Analysis:

The final stage of a penetration test is to compile the result by analyzing and commenting about the vulnerabilities exploited, access to the data, and the amount of time that the tester can remain unnoticed in the system.

# Ethical Hacking - Tools

## NMAP

## Metasploit

## Burp Suit

## Angry IP Scanner

## Network Stumbler

## ToneLoc

# Ethical Hacking - Skills

As an ethical hacker, you will need to understand various hacking techniques such as −

* Password guessing and cracking
* Session hijacking
* Session spoofing
* Network traffic sniffing
* Denial of Service attacks
* Exploiting buffer overflow vulnerabilities
* SQL injection

**Ethical hacking Vs Penetration testing**

