# Introduction to Ethical Hacking

**Hacker**

It is defined as the process in which the hacker uses the advantages of the vulnerabilities of the system to penetrate/intrude into the system

**Ethical hacking**

Ethical hacking contains methods to find vulnerabilities in a system and perform exploit to intrude/Penetrate in a system in legal way.

## Terminologies

**Attack**

An attack is an action that is done on a system to get its access and extract sensitive data

**Vulnerability**

weakness in a system eg: in hardware or software

**Exploit**

A method to intrude or penetrate in a system

**Payload**

Malicious code inside the exploit is called payload

**Malware**

Malware is malicious(intent ended to do harm) software which when enters the target host, gives an attacker full or limited control over the target

**Backdoor**

A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections

**Hack value**

The notion among hackers that something is worth doing. It is the reputation of the hackers  (i.,e) how good he is in hacking

**Zero day attack**

when a hacker finds a new vulnerability in a system and no one others know about it , that vulnerability or exploit is called zero day attack

**Firewall**

A firewall is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules

**Intrusion Detection & Intrusion Prevention**

IDS/IPS compare network packets to a cyberthreat database containing known signatures of cyberattacks. The main difference between them is that IDS is a monitoring system, while IPS is a control system

# Hacker Classes

**Black hat hackers**

The hacker who have excellent computing skills and the most talented hackers in the world.

They do hack for illegal purpose. That’s why they are called black hat hackers.

**White hat hackers**

They are professional hackers who work in the industry

They are also called ethical hackers

They work for legal purpose, companies hire white hat hackers

**Grey hat hackers**

These hackers work both sides legal as well as illegal

**Suicide hackers**

They don’t care about the result of hacking

They just want to hack the system and they don’t bother about prison

**Script kiddies**

These hackers are beginners in the hacking industry they are not familiar of any programming skills and just run the software tools created by others.

# Measures of security testing

**Confidentiality**

It protects against disclosure of sensitive information to the unintended recipients

**Integrity**

It allows transferring correct and accurate information from senders to intended receivers

**Authentication**

It verifies and confirms the user identity

**Authorization**

Specifies access rights to the users and resources

**Availability**

It specifies the readiness of the information on requirement

**No-repudiation**

It ensures that no denial of service from sender or receiver

**Vulnerability Assessment**

It is a process of identifying vulnerabilities/loopholes/weakness in the computer systems, networks and the communication channels

Blue Team

**Penetration testing**

It is the process of taking control over the system using the vulnerabilities identified in the vulnerability assessment phase

Red Team

**Security Audit**

Security audit check whether the organization is working under proper security policies/standards/laws

# Methodology