**Ethical hacking** is the practice of legally and systematically testing computer systems, networks, or applications to identify vulnerabilities, weaknesses, or security flaws that malicious hackers could exploit. Ethical hackers, often called "white hat hackers," work with the permission of the system owner to improve security and protect against potential cyberattacks.

**Key Aspects of Ethical Hacking:**

**Legal Authorization**: Ethical hackers must have explicit permission from the system owner before conducting any tests.

**Purpose**: The primary goal is to improve security by finding and fixing vulnerabilities before malicious hackers can exploit them.

**Techniques**: Ethical hackers use the same methods and tools as malicious hackers but operate within an ethical and legal framework.

**Reporting**: After testing, ethical hackers provide detailed reports outlining the vulnerabilities discovered, their potential impact, and recommendations for remediation.

**Tools of an ethical Hacker.**

Automatic tools have changed the world of penetration testing/ethical hacking, IT security researcher has been developed and currently developing different tools to make the test fast, reliable and easier task. Without automatic tools, the hacking process is slow and time consuming. The best tools that are widely used in the world of hacking are:

* **Nmap** is a best tool ever that are used in the second phase of ethical hacking means port scanning, Nmap was originally command line tool that has been developed for only Unix/Linux based operating system but now its windows version is also available and ease to use. It is use for Operating system fingerprinting too
* **Nessus** is the world most famous vulnerability scanner, Nessus has been developed by Tenable network security, it is available for free of cost for non-enterprise environment means for home user. It is a network vulnerability scanner used for finding the critical bugs on a system.
* **Nikto** is a free and open-source tool, It checks for outdated versions of over 1000 servers, and version specific problems on over 270 servers, It find out the default files and programs. It is a best tool for web server penetration testing.
* **Kismet** Wardriving or Wireless LAN(WLAN) hacking is in market and different companies hire penetration tester for doing test on wireless network, this test requires some tools, so Kismet is a best choice to do this. Kismet identifies networks by passively collecting packets and detecting networks, which allows it to detect hidden networks and the presence of non- beaconing networks via data traffic.

**Techniques of ethical hacking:**

***Information gathering***.

In this stage, The testers collect as much information about the web application as possible and gain understanding of its logic. The deeper the testers understand the test target, the more successful the penetration testing will be. The information gathered will be used to create a knowledge base to act upon in later steps. The testers should gather all information even if it seems useless and unrelated since no one knows at the outset what bits of information are needed. This step can be carried out in many different ways: by using public tools such as search engines; using scanners; sending simple HTTP requests or specially crafted requests or walking through the application.

# Vulnerability Analysis

Using the knowledge collected from the information gathering step, the testers then scan the vulnerabilities that exist in the web application. The testers can conduct testing on configuration management, business logic, authentication, session management, authorization, data validation, denial of service, and web services [4]. In this step, web server vulnerabilities, authentication mechanism vulnerabilities, input-based vulnerabilities and function-specific vulnerabilities are examined.

Vulnerability scanning

Exploitation

Test Analysis