# Ethical Hacker Methodology

## The Five Stages of Ethical Hacking

Ethical hacking, or penetration testing, follows a structured approach to identify and address vulnerabilities in computer systems and networks. The ethical hacking process typically involves the following five stages:

### Reconnaissance:

The reconnaissance stage involves gathering information about the target. It includes passive information gathering techniques like searching publicly available information, browsing websites, and examining DNS records. The goal is to collect as much information as possible to understand the target and identify potential entry points.

### Scanning:

In the scanning stage, you actively probe the target to discover open ports, services, and vulnerabilities. Various tools and techniques are used, such as port scanning, network mapping, and vulnerability scanning. This stage helps identify potential weaknesses that can be exploited.

### Gaining Access:

In this stage, you attempt to gain unauthorized access to the target. The focus is on exploiting vulnerabilities found during the scanning stage. Techniques like password cracking, social engineering, and exploiting software vulnerabilities may be used to gain access to the target.

### Maintaining Access:

Once access is gained, you should aim to maintain access to the compromised target. This stage involves bypassing security mechanisms, setting up backdoors or remote access tools, and establishing persistent access. The objective is to mimic the actions of a real attacker and assess the potential impact of a successful compromise.

### Covering Tracks:

In the final stage, you remove any traces of the activities performed against the target. This includes deleting logs, modifying/removing files, and restoring the system to its original state. The goal is to ensure that the activity remains undetected, leaving no evidence of the penetration testing activity behind.

It's important to note that ethical hacking should always be performed with proper authorization and within the bounds of the law. Ethical hackers are responsible for following strict ethical guidelines, maintaining confidentiality, and obtaining necessary permissions from the system or network owners before conducting any penetration testing activities.