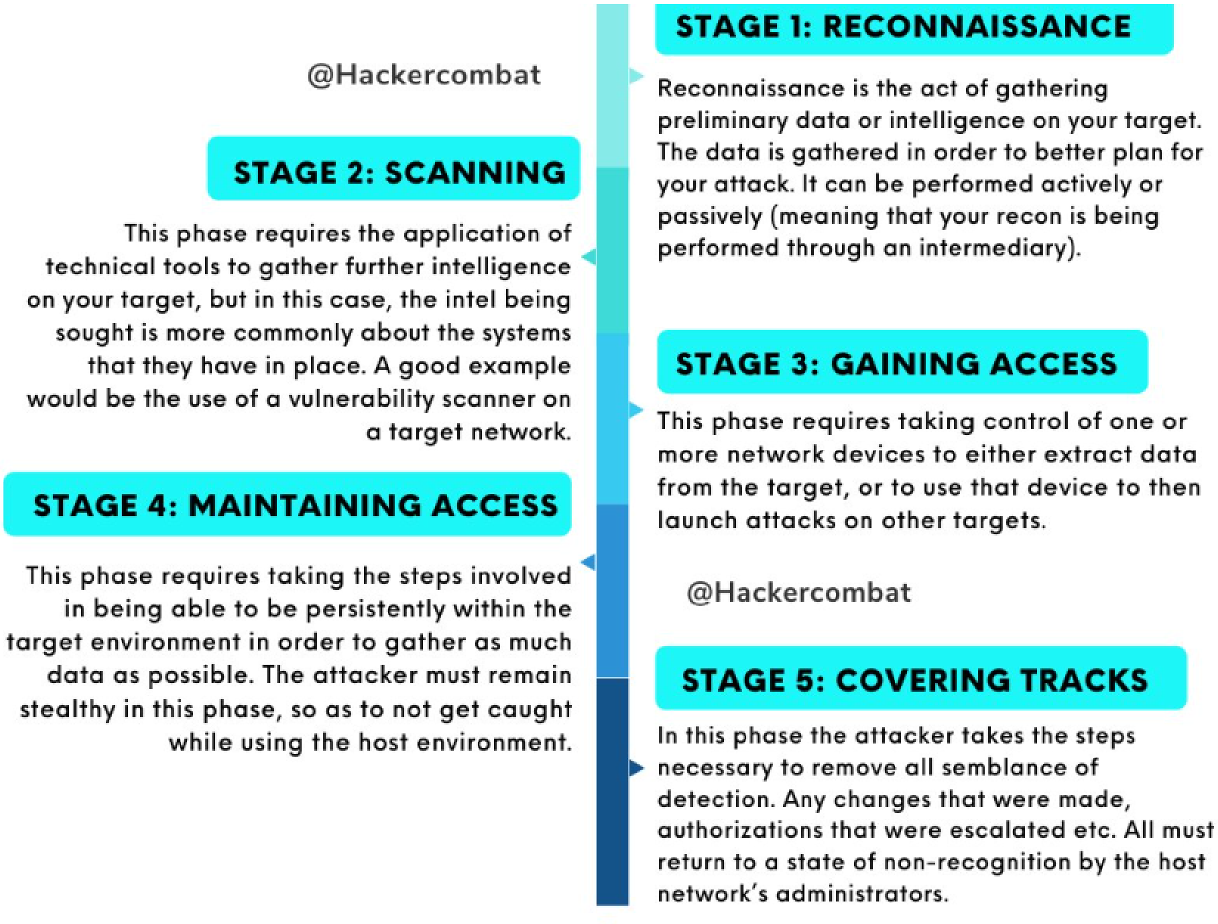
Phases of Hacking

There are mainly **5 phases in hacking**. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It’s a stepwise process and when followed yields a better result.

1. *Reconnaissance*
2. *Scanning*
3. *Gaining Access*
4. *Maintaining Access*
5. *Clearing Tracks*



STAGE 1: RECONNAISSANCE

Reconnaissance is the act of gathering preliminary data or intelligence on your target. The data is gathered in order to better plan for your attack. It can be performed actively or passively (meaning that your recon is being performed through an intermediary).

STAGE 2: SCANNING

This phase requires the application of technical tools to gather further intelligence on your target, but in this case, the intel being sought is more commonly about the systems that they have in place. A good example would be the use of a vulnerability scanner on a target network.

STAGE 3: GAINING ACCESS

This phase requires taking control of one or more network devices to either extract data from the target, or to use that device to then launch attacks on other targets.

STAGE 4: MAINTAINING ACCESS

This phase requires taking the steps involved in being able to be persistently within the target environment in order to gather as much data as possible. The attacker must remain stealthy in this phase, so as to not get caught while using the host environment.

STAGE 5: COVERING TRACKS

In this phase the attacker takes the steps necessary to remove all semblance of detection. Any changes that were made, authorizations that were escalated etc. All must return to a state of non-recognition by the host network’s administrators.

Let’s discuss a short intro about these 5 phase.

1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

1. Network
2. Host
3. People involved

There are **two types of Footprinting**:

Active: Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target

Passive: Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

While there are several tools available, here are a few **popular ethical hacking tools** commonly **used during the scanning phase**:

- SNMP Sweepers
- Ping sweeps
- Network mappers
- Vulnerability scanners

3. Gaining Access

Once ethical hackers expose vulnerabilities through the process's first and second hacking phases, they now attempt to exploit them for administrative access. The third phase involves attempting to send a malicious payload to the application through the network, an adjacent subnetwork, or physically using a connected computer. Hackers typically use many hacking tools and techniques to simulate attempted unauthorized access, including:

- Buffer overflows
- Phishing
- Injection attacks
- XML External Entity processing
- Using components with known vulnerabilities

If the attacks are successful, the hacker has control of the whole or part of the system and may simulate further attacks such as data breaches and Distributed Denial of Service (DDoS).

4. Maintaining Access

The fourth phase of the ethical hacking process involves processes to ensure the hacker can access the application for future use. A white-hat hacker continuously exploits the system for further vulnerabilities and escalates privileges to understand how much control attackers can gain once they pass security clearance. Some attackers may also try to hide their identity by removing the evidence of an attack and installing a backdoor for future access.

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. **This can be done using** Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

5. Clearing Tracks

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him.

To avoid any evidence that leads back to their malicious activity, hackers perform tasks that erase all traces of their actions. These include:

- Uninstalling scripts/applications used to carry out attacks
- Modifying registry values
- Clearing logs
- Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

- Tunneling
- Stenography

Having successfully performed all the 5 steps of ethical hacking, the ethical hacker then concludes the steps of ethical hacking by documenting a report on the vulnerabilities and suggesting remediation advice.