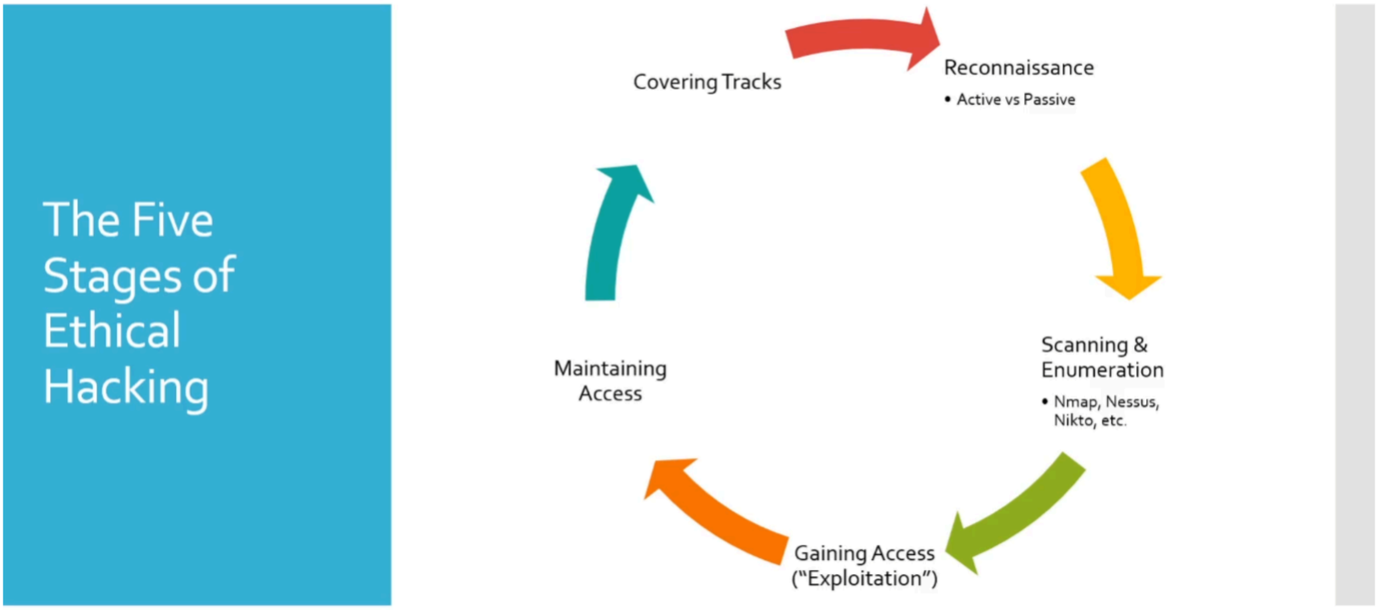
The Five Stages



The Five Stages of Ethical Hacking

Reconnaissance
- Active vs Passive

Scanning & Enumeration
- Nmap, Nessus, Nikto, etc.

Gaining Access ("Exploitation")

Maintaining Access

Covering Tracks

Passive is going to google, linked profiles, looking for pictures... . It is also known as information gathering.

Active falls into what is also called " Scanning & Enumeration". Probing the system directly.

Overall Picture

Ethical hacking, also known as penetration testing or white-hat hacking, 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 system or network. It includes passive information gathering techniques such as 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, the ethical hacker actively probes the target system or network to discover open ports, services, and vulnerabilities. Various tools and techniques are employed, such as port scanning, network mapping, and vulnerability scanning. This stage helps identify potential weaknesses that can be exploited.

Gaining Access:

In this stage, the ethical hacker attempts to gain unauthorized access to the target system or network. The focus is on exploiting vulnerabilities discovered during the scanning stage. Techniques such as password cracking, social engineering, and exploiting software vulnerabilities may be employed to gain access to the target system.

Maintaining Access:

Once access is gained, the ethical hacker aims to maintain access to the compromised system or network. 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, the ethical hacker removes any traces of their activities from the target system or network. This includes deleting logs, modifying or removing files, and restoring the system to its original state. The goal is to ensure that the ethical hacking 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.