MITRE ATT&CK SUMMARY

What is the MITRE ATT&CK :

MITRE ATT&CK is a framework that documents attack phases and tactics in the field of cyber security and has become an international standard. This framework describes in detail the methods used by cyber attackers and provides an important resource for creating defense strategies.

Main stages:

- **Reconnaissance(TA0043):** Reconnaissance consists of techniques that involve enemies actively or passively gathering information that can be used to support targeting.
- **Initial Access(TA0001):** Is the phase where an attacker tries to gain the first entry point into a network.
- **Persistence(TA0003):** The attacker becomes permanent in the system
- **Privilege Escalation(TA0004):** The attacker is trying to gain higher-level permissions.
- **Discovery(TA0007):** The attacker explores within the system.
- **Collection(TA0009):** The attacker is trying to gather data of interest to their goal.
- **Command and Control(TA0011):** The attacker is trying to communicate with compromised systems to control them.
- **Impact(TA0040):** The attacker is trying to manipulate, interrupt, or destroy your systems and data.

Some important tactics:

- **Spearphishing Attachment(T1566.001):** In short, it aims to gain access to the system by tricking the victim with malicious files attached to fake emails written with a focus on deception.
- **Exploitation for Client Execution(T1203):** Is a phase where attackers attempt to execute code using software vulnerabilities in client applications. These vulnerabilities can occur in software due to insecure coding practices and can lead to unexpected behavior.
- **Scheduled Task/Job(T1053):** With Scheduled Task, the attacker can set the malicious code to run automatically at a specific time. With this method, he can provide himself with persistence.
- **Hijack Execution Flow(T1574):** **Hijack Execution Flow** is a phase where attackers attempt to execute their own malicious code by hijacking how operating systems run programs. This is used by the attacker to gain access to the target, elevate privileges or bypass defense mechanisms.
- **Data Manipulation(T1565):** By manipulating data, attackers can hide their own activities, lead the target organization to make wrong decisions, sabotage a project.
- **Financial Theft(T1657):** The attacker may demand a ransom, steal credit card information or commit fraudulent activities through the system for their own financial gain.