MITRE ATT&CK FRAMEWORK

INDEX:

What is MITRE ATT&CK framework

The MITRE ATTACK Framework is a well-chosen knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle. The framework is meant to be more than a collection of data: it is intended to be used as a tool to strengthen an organization's security posture.

Here are three iterations of MITRE ATT&CK:

1. **ATT&CK for Enterprise**: Focuses on identifying and imitating adversarial behaviour in Windows, Mac, Linux, and cloud environments.
2. **ATT&CK for Mobile**: Focuses on identifying and imitating adversarial behaviour in Android and iOS operating systems.
3. **ATT&CK for ICS**: Focuses on describing the actions adversaries might take when they operate in an industrial control system (ICS).

What I Understand

- While learning cyber security concepts and different types of attack I so many times thinks that how can I manage to understand these many attacks and after understanding all attacks techniques how can I manage these much attack which attack when to apply, what should be specific order, how can I verify my order is right etc...

- Then in one lecture I got information about what is mitre att&ck framework, so what I understand is mitre att&ck framework is one stop solution of all my above-mentioned questions.

- MITRE ATT&CK framework is collection of all techniques and their tactics that attacker can used to exploit target machine.

- Main specialty is that all techniques and tactics are arranges in specific matrix form.

- This proper form helps to understand specific chain to do attack.

So finally, now I can identify different types techniques and its tactics that can I use to do attack. By using customization, I can also create my own proper step by step techniques based on available framework.

Why it is Important

As previously mentioned, there are three types of frameworks

- One is "**ATT&CK for Enterprise**" that useful for organizations and individual also because both may use one of four windows or Linux or macOS or cloud environment.

- Let us say Organization know about most dangerous attack so organization may know how attack can be done but they may do not know all techniques about that attack.

- So, they can use this **ATT&CK for Enterprise** framework to get more knowledge about all techniques and tactics, so now they in how many different ways the attack can be done on organization so they can highly mitigate attack risk on company.

- For example, in att&ck framework there is technique called Reconnaissance one sub-technique is Purchase Technical Data:
  Adversaries may purchase technical information about victims that can be used during targeting. Information about victims may be available for purchase within reputable private sources and databases, such as paid subscriptions to feeds of scan databases or other data aggregation services.

- So now organization can apply more security on their private data so that private recourses cannot get it from anywhere.

One more very interesting feature is →

You can customize matrix as you want using attack navigator, after that you can download that matrix and can store in your computer.

These feature is very useful when you need to upload mind map like image on your project or in presentation or education purpose etc.