This is a short introduction to the MITRE ATT&CK Framework. Keep in mind that everything about the MITRE ATT&CK Framework cannot be condensed in one blog, but reading this will help you get familiar with the basics of the Framework and put you on a path where you can research more about it on your own, which I highly recommend.

Objectives:

- **The Problem**
- **An Introduced Solution**
- **What is it**
- **How does it help**
- **Tactics used in ATT&CK**
- **Online Training**
- **Certifications**

THE PROBLEM

With the fast pace of growing technology in this day and age, It is hard to keep up with all the latest exploits / vulnerabilities found in technology and it is even harder to track how adversaries (one person or a group of people whose intentions are to perform malicious actions) use sophisticated techniques to take advantage of vulnerabilities (flaws / weakness) in applications.

AN INTRODUCED SOLUTION

With this rising problem in mind, The MITRE Corporation (American non-profit organization that supports U.S. government agencies in defense, healthcare, cybersecurity, etc.) introduced the ATT&CK® Framework. ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge). Some terms that you want to you familiarize yourself with before continuing:

- Tactic: The goal of the adversary

- Technique: The steps used by adversaries to achieve their goal
- Procedure: How the technique they use is carried out

What is the MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a constantly growing knowledge base of tactics, techniques and procedures that have been studied from countless adversarial attacks on company infrastructures / networks. It was initially an internal project known as FMX (Fort Meade Experiment). It soon was a globally accessible gold mine that many security vendors have picked up. It is built from publicly reported cyber activities and anyone can help contribute to it.

How does it help

It can be used as a guide for security professionals to map what attack techniques sophisticated hacker / hackers groups use, and using that information to help make better defensive decisions. It helps connect TTPs to threat actors and malware / tools that they use.

Tactics Used in ATT&CK

Each of these tactics have multiple techniques, this section will give you a short definition of each of the tactics, I highly recommend you researching them on your own and looking at all the techniques on a high level

- Initial Access
    - Gaining an initial foothold on the network. Techniques such as Phishing and Exploiting Public Facing Applications are commonly used to get access into a network / machine.
- Execution
    - The execution phase is where the adversary is trying to *execute* code on the machine / network. They are trying to get a shell (a command line interface that you can use to interact with the network / machine using commands) on the network.
- Persistence

    - Trying to maintain continuous access to the network / machine so that the adversary can come back and still have access to the network.
- Privilege Escalation
    - Trying to gain higher-level permissions / access on the network, an example could be changing your permissions from just being able to see files that are only accessible to common users to being able to access administrator files that are way more sensitive.
- Defense Evasion
    - Techniques adversaries use to bypass / avoid detection while they conduct their engagement
- Credential Access
    - Stealing credentials (usernames and passwords)
- Discovery
    - Gaining knowledge about the network and the overall infrastructure
- Lateral Movement
    - Trying to get into other user accounts with usually the same level permissions as the current user the
    - adversary has compromised
- Collection
    - Collecting information that the adversary sees important and that also helps their goal
- Command and Control
    - Techniques that are used by adversaries for communicating with the compromised systems
- Exfiltration
    - Basically stealing data
- Impact
    - Wreaking havoc to destroy data of the company

Online Training

A list of resources that you can use to get familiar with ATT&CK and practice using it

MITRE: TryHackMe Room: https://tryhackme.com/room/mitre
Using ATT&CK for Cyber Threat Intelligence Training:
https://attack.mitre.org/resources/training/cti/
MITRE ATT&CK Defender (MAD) ATT&CK Fundamentals Badge Training:
https://app.cybrary.it/browse/course/mitre-attack-defender-mad-attack-fundamentals

Certifications

ATT&CK Cyber Threat Intelligence Certification:
https://mad-certified.mitre-engenuity.org/group/283476