MITRE ATT&CK Framework

Table of contents:

Introduction to MITRE ATT&CK:

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Created by the MITRE Corporation, ATT&CK is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

The framework was introduced in 2013 and has since become a crucial tool in understanding how cyber attackers operate, providing a detailed view of the tactics, techniques, and procedures (TTPs) used by adversaries. The ATT&CK knowledge base is continually updated based on contributions from the cybersecurity community, making it a living document that evolves with emerging threats.

MITRE ATT&CK catalogs cybercriminal tactics, techniques and procedures (TTPs) through each phase of the cyberattack lifecycle—from an attacker's initial information gathering and planning behaviors, through to the ultimate execution of the attack. The information in MITRE ATT&CK can help security teams

MITRE ATT&CK Enterprise Techniques:

The Enterprise matrix within MITRE ATT&CK is one of the most widely used matrices, specifically focusing on techniques that adversaries use to compromise and maintain access to enterprise environments. It includes tactics like Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, and Impact.

- **Initial Access**: Techniques like phishing and exploiting public-facing applications to gain a foothold in the network.
- **Execution**: Methods like PowerShell scripting or command-line interfaces used to run malicious code.
- **Persistence**: Techniques like creating new accounts or modifying system processes to maintain access after a reboot.
- **Privilege Escalation**: Methods to gain higher-level permissions, such as bypassing user account control.
- **Defense Evasion**: Techniques to avoid detection, including disabling security tools or obfuscating code.
- **Credential Access**: Methods to steal credentials, like keylogging or credential dumping.
- **Discovery**: Techniques to gather information about the network environment, such as network scanning.
- **Lateral Movement**: Techniques to move through the network, like using remote services or pass-the-hash.
- **Collection**: Methods to gather data, such as keylogging or screen capture.
- **Exfiltration**: Techniques to steal data, like exfiltrating files over alternative protocols.

Use Cases of MITRE ATT&CK:

MITRE ATT&CK has several critical use cases in cybersecurity:

1. **Threat Intelligence: ** ATT&CK is used to analyze and map threat intelligence reports, helping organizations understand the techniques used by specific adversary groups. This enables organizations to prioritize defenses against the most relevant threats.

2. **Red Teaming and Penetration Testing: ** ATT&CK provides a blueprint for red teamers and penetration testers to simulate real-world adversary behavior, ensuring that security defenses are tested against the tactics and techniques most likely to be employed in an actual attack.

3. **Integration with Security Tools: ** Many security tools and platforms integrate with ATT&CK to enhance detection, response, and threat hunting capabilities. By aligning security operations with the ATT&CK framework, organizations can better detect, mitigate, and respond to attacks.