MITRE ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is **a comprehensive knowledge base that categorizes the tactics, techniques, and procedures (TTPs) used by attackers throughout the lifecycle of a cyberattack**. Developed by MITRE Corporation, ATT&CK helps cybersecurity professionals **understand and defend against adversarial behavior by mapping real-world attack techniques to the different phases of an attack**. The framework is widely used in threat modeling, detection, and incident response.

Key Components of the MITRE ATT&CK Framework:

1. **Tactics**:

- Tactics represent the goals or objectives an attacker aims to achieve at each **stage of an attack**. Each tactic aligns with a specific phase in the attack lifecycle, providing a high-level view of the attacker's goals.
- Examples of Tactics:
    - Initial Access: Gaining entry into the target network.
    - Persistence: Maintaining a foothold within the system.
    - Privilege Escalation: Obtaining higher access levels to perform unauthorized actions.
    - Lateral Movement: Moving through the network to find additional targets.
    - Exfiltration: Stealing data from the system.

2. **Techniques**:

- Techniques describe **the specific methods or actions attackers use to achieve their objectives within each tactic**. Techniques provide detailed descriptions of how adversaries can compromise systems, evade detection, and achieve their goals.
- Examples of Techniques:
    - Phishing (Initial Access): Using email to deceive users into downloading malware or disclosing credentials.
    - Credential Dumping (Credential Access): Extracting stored passwords or hashes from a system to facilitate unauthorized access.
    - Remote File Copy (Lateral Movement): Transferring files from one host to another to establish control over new systems.
    - Data Compression (Exfiltration): Compressing files to reduce their size before exfiltrating data out of the target network.

3. **Sub-Techniques**:

- Sub-techniques break down each technique into **more specific actions, providing a more granular level of detail**. Sub-techniques allow organizations to understand the exact methods attackers might use under each main technique.
- Example of a Technique with Sub-Techniques:
    - Phishing (Initial Access) has sub-techniques like Spear Phishing Attachment (sending malicious attachments), Spear Phishing Link (sending malicious links), and Spear Phishing via Service (using a third-party service to deliver phishing messages).

4. **Procedures**:

- Procedures describe **specific, real-world implementations of techniques**. They document how different threat actors or malware families use certain techniques in actual attacks, providing context and examples of the techniques in action.
- Example: APT28 (a known threat group) using spear-phishing emails with malicious attachments to gain initial access to a target organization.

MITRE ATT&CK Matrices:

The MITRE ATT&CK framework provides multiple matrices that organize tactics and techniques according to different environments, such as:

- Enterprise: Focused on attacks against enterprise networks and systems, including Windows, macOS, Linux, and cloud environments.
- Mobile: Contains tactics and techniques specific to mobile platforms, including both Android and iOS.
- ICS (Industrial Control Systems): Focused on attacks against industrial and critical infrastructure systems, such as SCADA (Supervisory Control and Data Acquisition) and OT (Operational Technology) environments.

Each matrix is a structured table where the rows represent techniques and the columns represent tactics. This structure allows analysts to see how each technique aligns with a specific tactic in the attack lifecycle.

Common Use Cases for the MITRE ATT&CK Framework:

1. **Threat Detection and Response**:

- Security teams use ATT&CK to map observed attacker behavior to known techniques and tactics. By comparing suspicious activity to the framework, they can better understand the attack's progression and prioritize responses based on the attack's lifecycle stage.

2. **Threat Intelligence**:

- Threat intelligence teams use ATT&CK to profile threat actors by associating their known TTPs with tactics and techniques in the framework. This helps security teams anticipate future actions based on the attacker's profile.

3. **Incident Investigation and Forensics**:

- Investigators use ATT&CK to map out all the observed behaviors during an incident. This helps analysts understand how an attack was conducted and identify which techniques may have been used but weren't detected, highlighting potential gaps in defense.

4. **Red and Blue Teaming**:

- Red teams (offensive security teams) use ATT&CK to simulate realistic attack scenarios by mimicking techniques that real-world adversaries use. Blue teams (defensive teams) use the framework to prepare defenses and monitor for specific techniques in their environment.

5. **Security Gap Analysis**:

- Organizations can use ATT&CK to evaluate their current security controls and see if they are adequately covering known techniques. This helps in identifying potential gaps and implementing additional security measures to cover them.

Example of an ATT&CK Matrix Row:

Here's a simplified example of a row in the MITRE ATT&CK Enterprise Matrix, focused on the "Initial Access" tactic:

Tactic	Technique	Sub-Technique	Procedure (Example)
Initial Access	Phishing	Spear Phishing Attachment	APT28 uses malicious attachments in emails to gain access to target networks
Initial Access	Exploit Public-Facing Application	N/A	Attackers exploit unpatched vulnerabilities in web servers to gain entry
Initial Access	Drive-by Compromise	N/A	APT32 uses compromised websites to deliver malware to unsuspecting visitors

This row shows how techniques and sub-techniques are mapped to the "Initial Access" tactic, along with real-world examples of threat actors using these methods.

Summary:

The MITRE ATT&CK Framework is a widely used threat intelligence and defense framework that categorizes the tactics, techniques, and procedures (TTPs) used by attackers. The framework is structured into matrices that map tactics (the goals attackers aim to achieve) to techniques (the specific methods they use). It is used by cybersecurity professionals for threat detection, threat intelligence, incident response, and gap analysis, providing a common language and structured approach for understanding and defending against cyber threats.