MITRE ATT&CK® Overview: Key Tactics and Techniques

What is MITRE ATT&CK?

The **MITRE ATT&CK®** (Adversarial Tactics, Techniques, and Common Knowledge) framework is a globally accessible knowledge base of adversary behaviors. It acts as a comprehensive manual for cybersecurity professionals to understand, detect, and mitigate cyberattacks based on real-world observations.

Common Attack Types & Solutions

1. Phishing

- **Tactic:** Initial Access
- **Definition:** Phishing is the use of deceptive emails, websites, or messages to trick users into revealing sensitive information (like passwords) or downloading malware. It is the most common way attackers gain a foothold in a network.
- **Mitigation:** Implement **Multi-Factor Authentication (MFA)** across all accounts so that stolen passwords alone are insufficient for access. Conduct regular **Security Awareness Training** to help users recognize and report suspicious messages.

2. Command and Scripting Interpreter

- **Tactic:** Execution
- **Definition:** Attackers often use built-in system tools like PowerShell, Python, or the Windows Command Shell (cmd) to run malicious code. Because these tools are legitimate and used by IT staff, the malicious activity can easily blend in.
- **Mitigation:** Restrict script execution using **AppLocker** or **Windows Defender Application Control (WDAC)**. Ensure that only digitally signed scripts can run on critical systems.

3. Create or Modify System Process

- **Tactic:** Persistence
- **Definition:** To ensure they remain in the system even after a reboot, attackers will create new background services or modify existing ones. This allows their malware to launch automatically whenever the computer starts.

- **Mitigation:** Follow the **Principle of Least Privilege (PoLP)** by ensuring users do not have local administrative rights. Regularly audit system configuration changes and use Endpoint Detection and Response (EDR) to flag unauthorized service creation.

4. Indicator Removal

- **Tactic:** Defense Evasion
- **Definition:** Once an attacker is inside, they often try to hide their tracks by deleting system logs, browser history, or security alerts. This "wiping of the feet" makes forensic investigation much harder.
- **Mitigation:** Use **Centralized Logging**. By streaming logs to a separate, secure server in real-time, the data is preserved even if the attacker deletes the local copies.

5. Exfiltration Over C2 Channel

- **Tactic:** Exfiltration
- **Definition:** This is the final goal: moving stolen data out of the network. Attackers often hide the stolen data within their existing Command and Control (C2) traffic—which is the communication line between the infected machine and the attacker—to avoid detection by simple traffic filters.
- **Mitigation:** Implement **Data Loss Prevention (DLP)** tools to scan outbound traffic for sensitive data patterns. Monitor for unusual spikes in outbound network traffic, especially to unknown or suspicious IP addresses.

Summary

The MITRE ATT&CK framework allows security teams to move from a "reactive" mindset (waiting for an alert) to a "proactive" one. By understanding these techniques, you can identify the gaps in your own security and strengthen your defenses before an attack occurs.