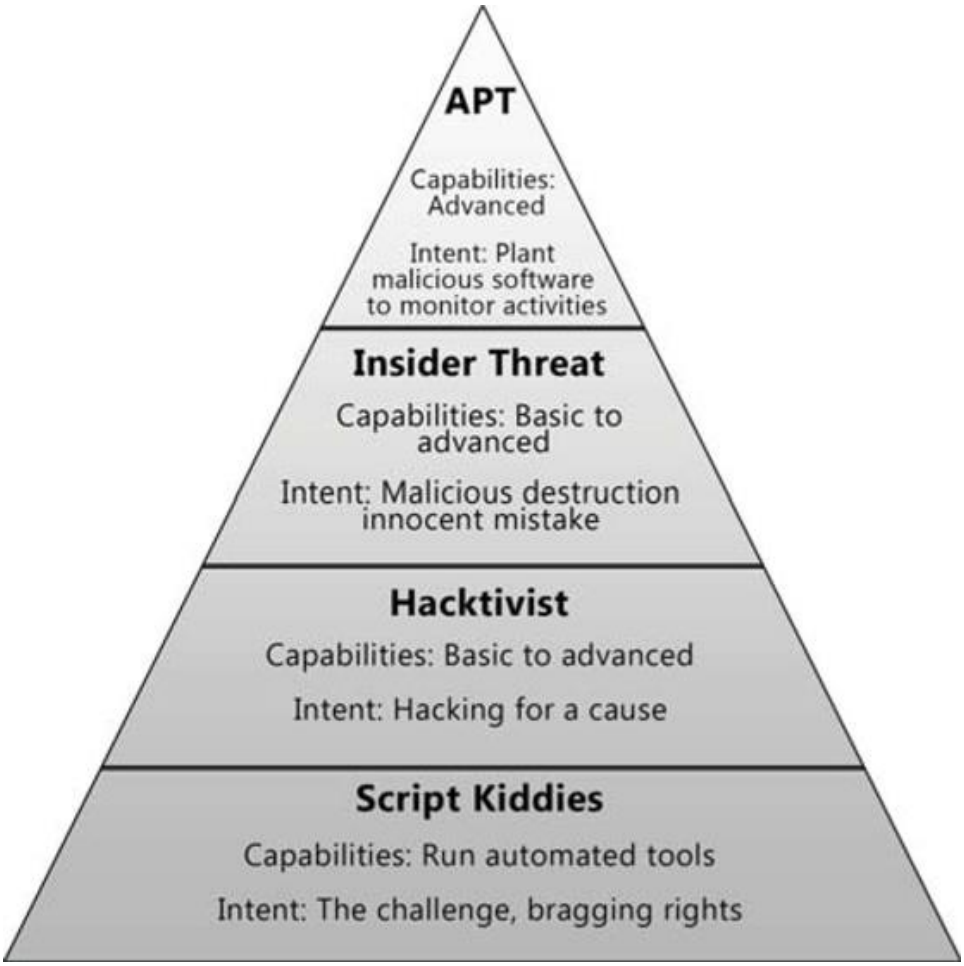
ADVERSARY TIERS IN PENETRATION TESTING



Penetration testing (pen testing) often involves simulating attacks from different types of adversaries. These adversaries are categorized by their skills, resources, and motivations, and are referred to as "adversary tiers." Understanding these tiers helps pen testers tailor their testing approach to reflect the most likely real-world threats an organization might face.

Common Adversary Tiers:

- **Tier 1: Script Kiddie/Opportunist**
    - **Description:** This tier represents individuals with limited technical skills who rely on readily available automated tools and exploits. They often target low-hanging fruit and easily exploitable vulnerabilities.
    - **Motivation:** May be motivated by vandalism, curiosity, or stealing readily available data.
    - **Pen Testing Approach:** Pen testers in this tier focus on identifying basic vulnerabilities like unpatched systems, weak passwords, and misconfigured web applications.
- **Tier 2: Script Kiddie with Malicious Intent**
    - **Description:** Similar to Tier 1, but with a more malicious intent. They might possess slightly more technical knowledge and may target specific vulnerabilities for personal gain (e.g., stealing financial information).

    - **Motivation:** Financial gain, identity theft, or causing disruption.
    - **Pen Testing Approach:** This tier expands on Tier 1, also testing social engineering techniques (tricking users) and exploiting common application vulnerabilities.

- **Tier 3: Insider Threat**
    - **Description:** This tier represents disgruntled employees, contractors, or anyone with authorized access who may misuse their privileges. They have insider knowledge about the system and its weaknesses.
    - **Motivation:** Revenge, financial gain, or leaking sensitive information.
    - **Pen Testing Approach:** This tier focuses on simulating attacks from authorized users, testing access controls, data exfiltration techniques, and privilege escalation vulnerabilities.

- **Tier 4: Advanced Persistent Threat (APT)**
    - **Description:** Highly skilled and well-resourced attackers with a persistent focus on a specific target. They employ sophisticated techniques and custom malware to gain access and remain undetected for extended periods.
    - **Motivation:** Espionage, intellectual property theft, or sabotage of critical infrastructure.
    - **Pen Testing Approach:** This tier involves advanced social engineering simulations, zero-day exploit testing (exploits for unknown vulnerabilities), and mimicking complex attack vectors used by APTs.

Benefits of Adversary Tiers:

- **Targeted Testing:** Allows focusing testing efforts on the most relevant threats based on the organization's risk profile.
- **Improved Security Posture:** Helps identify vulnerabilities that might be exploited by different types of adversaries.
- **Realistic Scenarios:** Provides a more realistic assessment of the organization's security posture.

Remember: Adversary tiers are a flexible framework. Pen testers should adapt their approach based on the specific needs of each engagement.