**SIKLUS DALAM MELAKUKAN PENYERANGAN**

CYCLE 1: In atau tahapan pertama untuk masuk

* Reconnaissance: Penyerang melakukan penelitian pada target menggunakan informasi yang tersedia untuk umum.
* Weaponisation: Menyiapkan infrastruktur yang diperlukan untuk menjadi tuan rumah pusat komando dan kendali (C2) sangat penting dalam melakukan serangan.
* Delivery: Muatan adalah instrumen jahat yang dikirim ke target melalui berbagai cara, seperti phishing email dan serangan rantai pasokan.
* Social Engineering: Penyerang akan mengelabui target mereka untuk melakukan tindakan tidak tepercaya dan tidak aman terhadap muatan yang baru saja mereka kirimkan, seringkali membuat pesan mereka tampak seperti berasal dari sumber internal tepercaya.
* Exploitation: Jika penyerang menemukan kerentanan yang ada, kelemahan perangkat lunak atau perangkat keras, dalam aset jaringan, mereka dapat menggunakan ini untuk memicu muatan mereka.
* Persistence: Penyerang akan meninggalkan kehadiran mundur di jaringan atau aset untuk memastikan mereka memiliki titik akses ke target mereka.
* Defence Evasion: Penyerang harus tetap anonim sepanjang eksploitasi mereka dengan menonaktifkan dan menghindari mekanisme pertahanan keamanan apapun yang diaktifkan, termasuk menghapus bukti kehadiran mereka.
* Command & Control: Ingat infrastruktur yang disiapkan penyerang? Saluran komunikasi antara sistem yang disusupi dan infrastruktur penyerang dibuat di internet.