Kill chains

task x

Kill chain cannot reach its preferred outcome without going through all the phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objectives. Even one mitigation can cause the kill chain to stop. This model essentially intrudes by gaining the opposers trust, establishing a presence on "enemy grounds", violating the CIA (**C**onfidentiality, **I**ntegrity and **A**vailability) in the system.

- reconnaissance: getting to know the opposition
- weaponization: finding the best way to deliver an automated tool
- delivery: automated tool is sent to opposition/target
- exploitation: intruders code is triggered in the system
- installation: a door to the system
- command and control: C2 channel possible through Internet controller server
- actions on objectives: access to do what they need to in the system remotely

task a

- Tactic: a way to perform an action
    - example: interrupting an attacks progress in a zero-day attack using vulnerability scanning
- Technique: how action is taken
    - example: reviewing the code and polishing it to prevent exploits from a zero-day exploitation
- sub-technique: more specific description of behavior to achieve a goal
    - example: in a session hijacking is session sniffing which means collecting data through insecure connections or guessing weak session IDs
- procedure: specific implementation of techniques and sub-techniques
    - example: session hijacker identifies the user first then attempt to gain access to their account

SOURSES:

- https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (3.2 Intrusion Kill Chain)
- https://attack.mitre.org/resources/faq/ (General)
- https://www.imperva.com/learn/application-security/zero-day-exploit/ (vulnerability detection)