3.2 Intrusion Kill Chain

Kill chain definition – a systematic process to target and engage a “victim” to obtain desired effects. According to the US Military, the process includes the following steps, known as F2T2EA

1. Find the target
2. Fix the location
3. Track and observe
4. Target with suitable weapon/asset
5. Engage the victim
6. Assess effects

The “chain” in the name implies the step-by-step nature of the process, as any failure in the sequence will interrupt the whole process.

The NEW model – CNA Computer Network Attack and CNE Computer Network Espionage intrusion kill chain is developed based on this concept and has the following phases:

1. Reconnaissance (Observation) – research phase, collecting information (emails, social relationship, info on specific technologies)
2. Weaponization – create a weapon (trojan) into a deliverable payload, such as Adobe PDF or MS Office documents.
3. Delivery – sending the payload to the targeted adversary, 3 most commonly used forms according to LM-CIRT in 2004-2010 are email attachments, websites and USB media.
4. Exploitation – triggering the code after delivery. Targets can be application or OS vulnerability, users themselves of OS feature leading to auto code execution.
5. Installation – installing remote access trojan/backdoor to maintain the existence of it at the victim environment.
6. Command and Control (C2) – usually the hosts must signal outbound to Internet controller server to establish a C2 channel rather over manual interaction than automatic. Once done, the intruders gain “hands on the keyboard” access inside the target environment.
7. Actions on Objects – the intruders take action to achieve their original goals. Usually, it’s data extraction (collecting, encrypting and extracting info), violation data integrity or availability, or using it as a hop point before moving further into the network.

3.3 Courses of Action   
Thorough understanding of intrusion kill chain model leads to the ability to build up measurement and decision to defend it. Defenders can also measure the performance and effectiveness of these actions as well as plan investment roadmaps to fix any existing gaps.

Table 1: Courses of Action Matrix showcases the actions (Detect, Deny, Disrupt, Degrade, Deceive, Destroy) over corresponding phases of intrusion kill chain listed in 3.2. The Matrix implies the importance of completeness of the actions *(“completeness equates to resiliency”) which* is the main goal of the defender over time.

Concept “zero-day attacks” and “zero day protection” are introduced*.*

Defender can “measure” its system resiliency by evaluating the performance and effectiveness of these actions as in fig.2 and based on that can have an overview or defending measures against intrusion attempts to locate the gaps and react accordingly.