Oefening 1:

Bij welke onderdelen van het Cyber Kill Chain Model kan er netwerkverkeer gegenereerd worden? Probeer ook een omschrijving te geven van het netwerkverkeer.

Oplossing:[i]

- Reconnaissance: Ping sweep, Nmap scan, TCP Reset, … .

- Weaponization: /

- Delivery: Connectie naar een website, download van een bestand, … .

- Exploitation: Connectie naar een specifieke host, mislukte aanmeldpogingen, …

- Installation: /

- Command and Control: C&C verkeer, RAT (Remote Access Tool) verkeer, …

- Actions on Objective: Data exfiltratie

[i] Belangrijke informatie: Deze oplossing is allesbehalve volledig!