## nmap

As the name suggests, nmap can be used to “map” a network, allowing the user to find potential connections to the client, often through the search of open ports or potentially vulnerable services.

***Possible Kill Chain Phases:***

- Reconnaissance – Nmap is primarily used in the initial reconnaissance phase to collect information about the target network. It helps identify live hosts, open ports, and services that could be exploited in future stages.

## hydra

Hydra is a logon cracking tool used to discover authentication credentials through a brute force method and can be used through various (frankly most) protocols.

***Possible Kill Chain Phases:***

- Delivery/Exploitation — If Hydra is used over a service like SSH, FTP, or HTTP, the tool directly engages with the target’s login interface to deliver brute force attacks. When successful, the crack itself could be an exploit, as Hydra helps the attacker exploit weak authentication mechanisms by gaining unauthorized access.

## sqlmap

Sqlmap is used to help find potential SQL injection vulnerabilities in web apps. Sqlmap provides many tools to then take advantage of these vulnerabilities, including various enumeration abilities, the ability to read files, or use custom SQL injection payloads.

***Possible Kill Chain Phases:***

- Exploitation — Sqlmap exploits known vulnerabilities in input fields or parameters linked to databases. It enables attackers to gather data or even take control of backend systems.

- Installation — If access is achieved through SQL injection, sqlmap can help an attacker plant web shells or backdoors into the system.

**The Krusty Krab Data Breach**

Plankton's back at it again… Tired of failed restaurant heists, he decides to go full black hat with a cyber attack to *finally* steal THE Krabby Patty Secret Formula. He boots up a terminal on Karen, his sentient robot wife, and get's started with an **nmap** scan of the Krusty Krab's network. Sure enough, he finds some open ports, including a *crusty* old FTP service and a customer feedback website. Plankton targets the FTP login using **hydra**, guessing Krabs probably uses something obvious like "money123" or "iloveca$h", so opts for his "most common passwords used by crabs" dictionary. After some brute forcing wait time, hydra cracks it with the combo: Krabs | green4life. Inside the FTP folders, Plankton finds a config file pointing straight to their main database server.

Rubbing his little green toothpick hands together, he heads to the feedback form on the website and fires up **sqlmap**. The form's wide open to SQL injection, and Plankton wastes no time. Before long, Plankton's downloading a database table called 'secret_recipes'. And there it is, the Krabby Patty Secret Formula.

**Assumptions: The Krusty Krab didn't secure their web forms or internal network, and apparently stores top secret recipes in plaintext. Additionally, the FTP server was misconfigured allowing hydra to brute force without lockouts, and an FTP service banner revealed the username "Krabs", or maybe Plankton had anonymous access and found a conveniently placed public file with the username. It's also assumed that the config file found via FTP gives him relevant context and target information to exploit the feedback form with sqlmap. And finally, the customer feedback form was outdated and vulnerable to classic SQL injection techniques. Just classic Krabs, cheaping out on cybersecurity.**