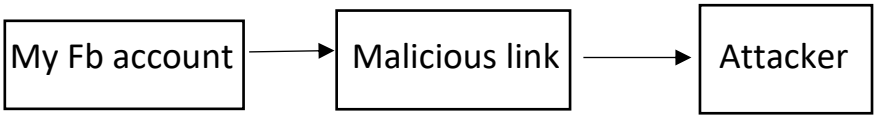
Introduction:

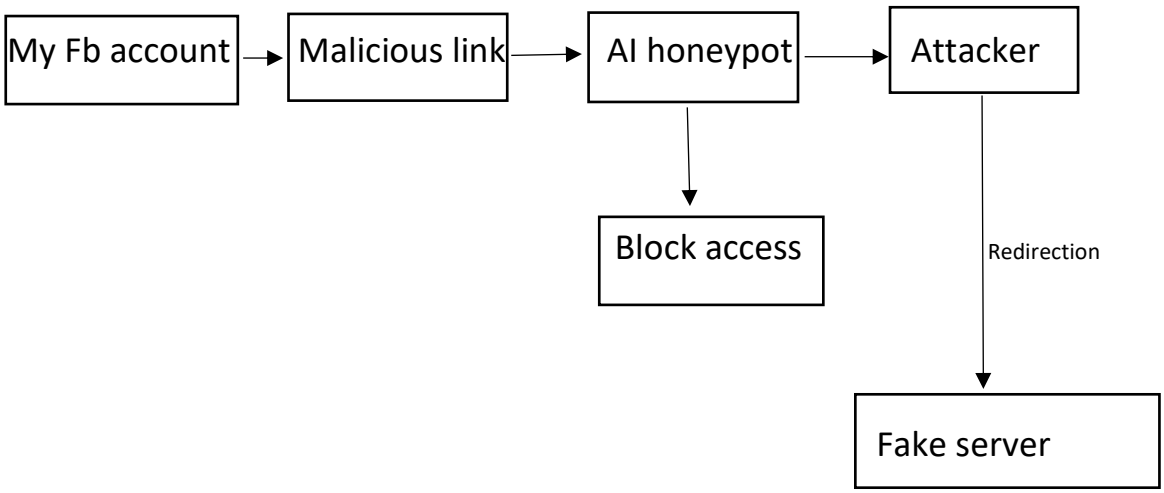
Most attackers target client's social media pages for mining confidential data and other malicious behavior. One of the most prevalent attacks for this purpose is phishing attack (Man in the Middle) which can be in form of fake likes, fake plugins or even fake offerings on one's social media web page.

Working of honeypot in network: Honeypots are a decoy tool to distract/redirect an attacker from the main priority information to a fake server giving him/her an impression of a successful attack.

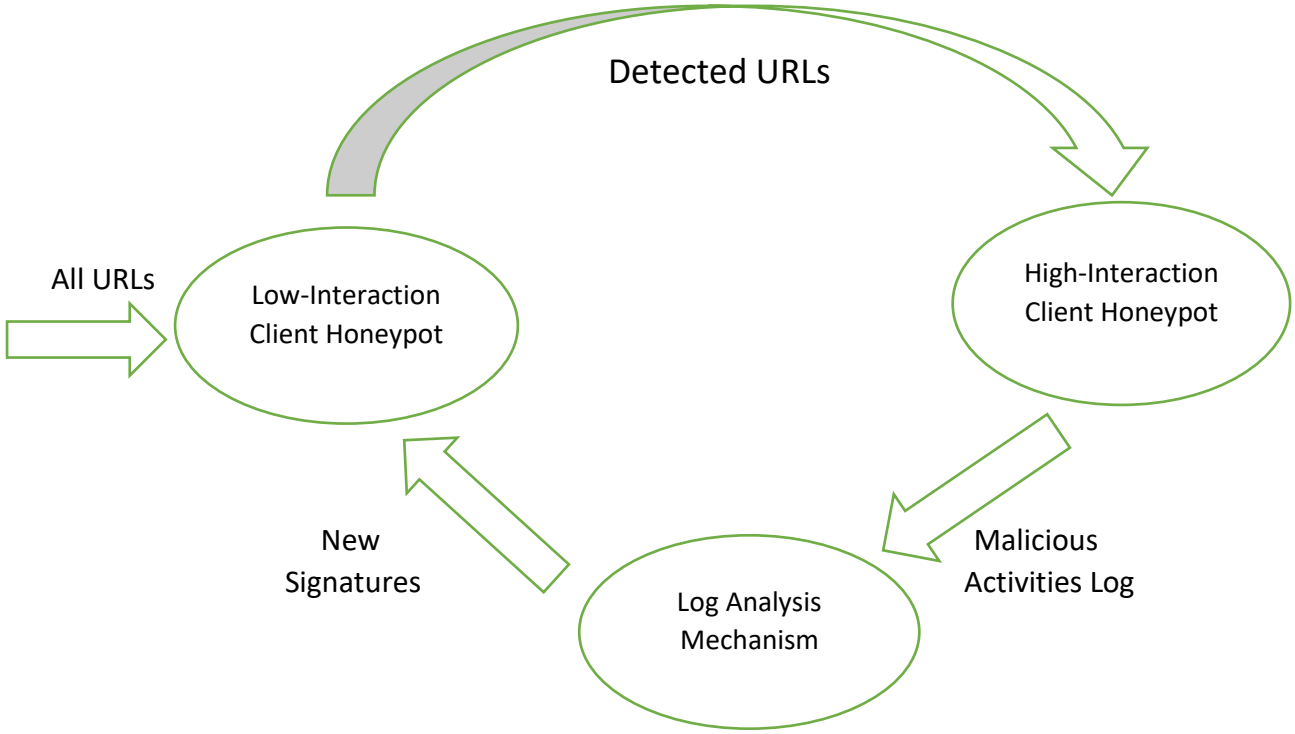
This happens:



Our Implementation:



Honeypot using AI block diagram:



Explanation of Analysis model:

Low Interaction Client Honeypot

- All URLs confront the Low Interaction Client Honeypot in the beginning where heuristic analysis is used to detect the malicious part of the code in the link by reading the source code. Heuristics refers to a set of rules as opposed to a specific set of program instructions used to detect malicious behaviour (basically reading the source code) without having to uniquely identify the program responsible for it (used in traditional methods).

High Interaction Client Honeypot

- Instead of redirecting it to the fake server, the link is forwarded to the high interaction honeypot to identify the type of malicious code/script is being used.
- Working of high interaction honeypot: Log files (For e.g. Capture tool) are used in the high interaction honeypot for performing K-means Clustering method to cluster different behaviors in categories/groups in order to study the similarity between all the malicious codes and create its own logs for new signatures used again, next time a new malicious URL is trying to penetrate the network.