*“She’s a malicious hooker.”*

**Mission:**

Intercept function calls to allow the modification of telemetry data, metadata, and all other non-user controlled data sent to a remote host in order to enable vulnerability scanning

**Search Terms:**

DLL Redirection/DLL Hijacking/Function Hooking/API Hooking

**Building a Local Intercepting Attack Proxy:**

* Use networking functions to identify call stacks
  + Rohitab API Monitor
* Intercept functions
  + Nektra Deviare API Hook
  + Record to a database
  + Parse all the everythings into tokens
* Capture network traffic using network functions
  + Parse everything and split
  + Intercept all the other functions and search for the traffic sent in the network
  + Find the call stacks and identify the plaintext that was put in
  + Wildcard the right things
    - Replay and record

Rip out the guts of ZAP Proxy

Redirect intercepted functions to ZAP

* Identify payload positions in functions
* Choose payload method
* Scan for technical vulnerabilities

Profit.

**Diagram:**



**To Do List:**

* ~~Intercept Windows function calls~~
* ~~Intercept and modify Windows function calls~~
* Frankenstein an attack proxy to intercept function calls
* Intercept networking functions and attack “Paranoid Mode” meterpreter
* Intercept other functions… and yolo sec
* Intercept android function calls
* Intercept and modify android function calls