Hiện nay mạng máy tính càng ngày càng phổ biến và đóng vai trò quan trọng trong đời sống của chúng ta. Chúng hiện hữu ở mọi nơi từ những chiếc laptop, điện thoại chúng ta sử dụng hàng ngày để tra cứu học tập đến hệ thống quản lý điểm học phần trong hệ thống nhà trường, học viện.

Việc mạng máy tính càng phát triển đồng nghĩa với việc chúng chứa nhiều các thông tin có giá trị quan trọng và trở thành mục tiêu tấn công của nhiều thành phần. Dẫn tới ngày càng có nhiều các cuộc tấn công xảy ra trên mạng máy tính.

Chúng ta không thể ngồi chờ đợi các cuộc tấn công xảy đến rồi mới tìm các biện pháp đối phó. Từ đó các công cụ kiểm thử được ra đời.

Mục tiêu đề tài của chúng em là xây dụ hệ thống sinh dũ liệu tấn công phục vụ mục đích kiểm thử các thiết bị mạng. Cụ thể hơn là tập trung tìm giải pháp cho việc tạo ra các công cụ kiểm thử dành riêng cho đối tượng đặc thù là hệ thống mạng LAN trong quân đội

Công tác kiểm thử hệ thống là sử dụng các công cụ cùng kỹ năng của bản thân để đưa vào hệ thống các input từ đó phát hiện ra những lỗi bất thường của hệ thống.

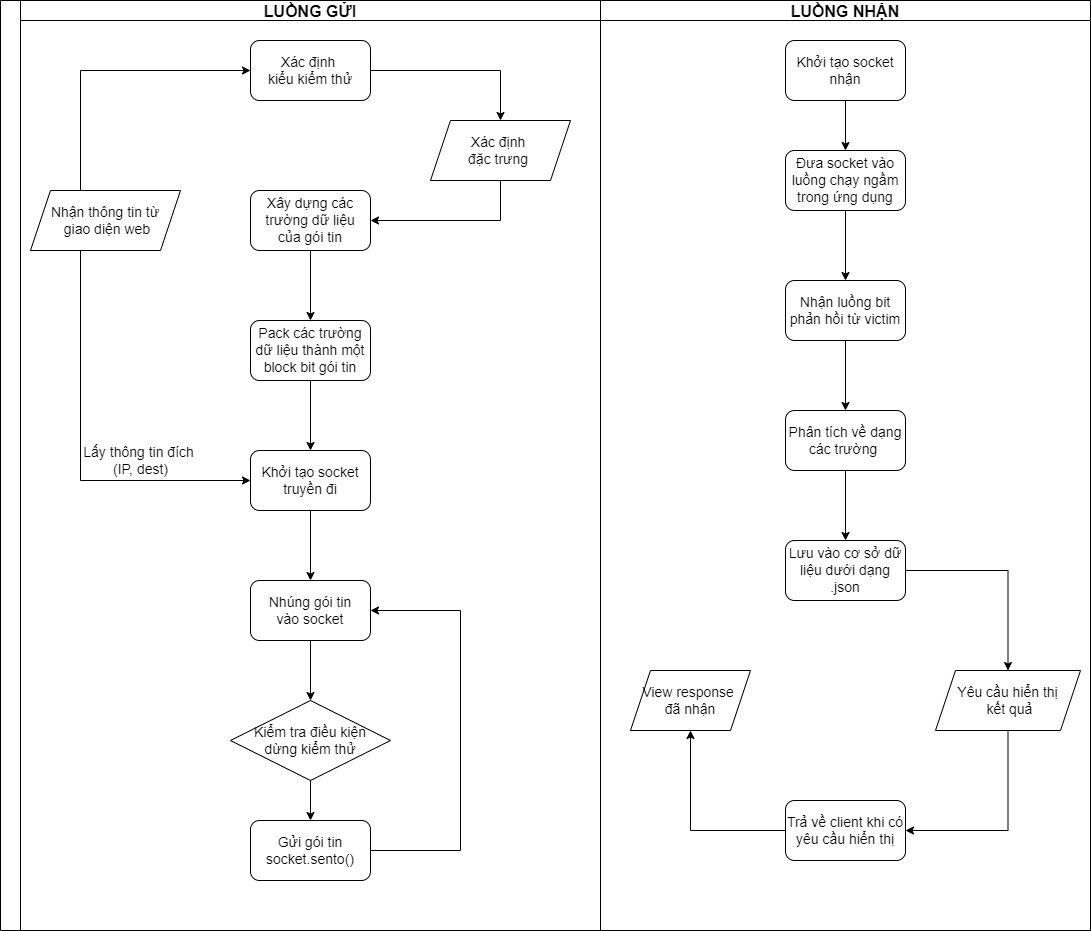
Hệ thống kiểm thử với vai trò tương tự nhưng giúp cho quá trình kiểm thử được nhanh chóng và chính xác hơn.

Mô hình OSI gồm 7 tầng và tầng thấp gồm 3-4 tầng dưới cùng

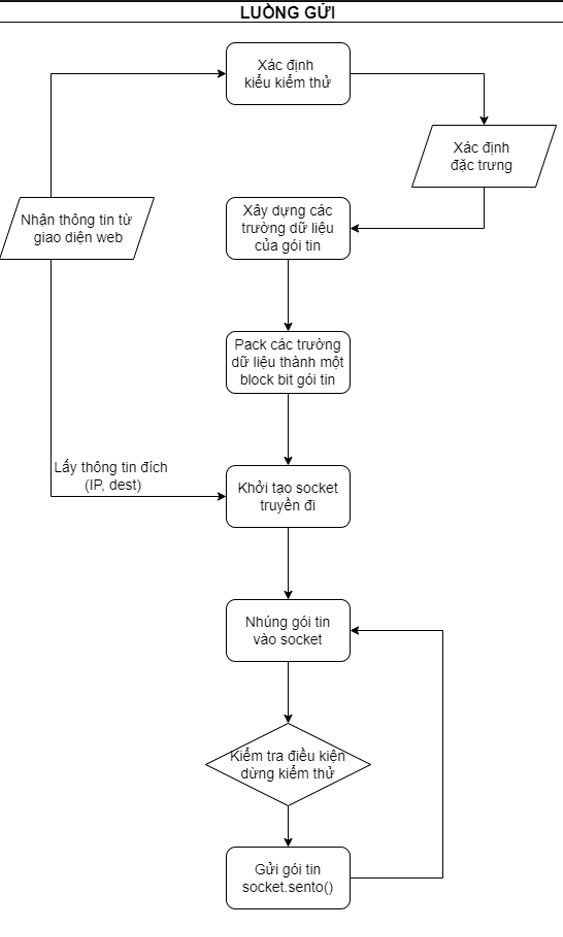
Tầng thấp có xu hướng khuyến khích truyền thông. Cùng với đó các giao thức bảo vệ thường tập trung nhiều vào application vì vậy những tầng này có thể coi là yếu nhất và dễ bị tấn công nhất

1. Socket là gì

* Là giao diện lập trình được sử dụng để truyền và nhận dữ liệu trong network. Trong quá trình truyển tải thông tin giữa hai hệ thống cần có một liên kết để hai hệ thống có thể tương tác với nhau. Và mỗi điểm cuối của liên kết này được gọi là socket.
* Socket giúp cho lập trình viên có thể giúp lập trình viên xây dựng gói tin của Layer 2, 3 một cách mặc định để truyền đi trong network. Tuy nhiên cách này là làm lập trình viên không thể cài đặt những yếu tố đặc thù của các gói tin tấn công.
* Socket cũng có thể giúp người dùng truyền tải một gói tin do người dùng tạo ra đến một địa chỉ cụ thể (thường gồm: Ip và port) với số lượng và tần suất khác nhau.
* Một module socket thường gồm 3 phần
* **socket\_family**: Đại diện cho họ địa chỉ (và giao thức). Nó có thể là AF\_UNIX hoặc AF\_INET, AF\_INET6
  + **AF\_UNIX**: Đại diện cho họ giao thức cục bộ.
  + **AF\_INET**: Vùng này sử dụng địa chỉ IP (cụ thể là Ipv4) để xác định kết nối vật lý. Ngoài ra chúng cũng có thể xử dụng để ánh xạ tới các địa chỉ IP qua Domain Name
  + **AF\_INET6**: Tương tụ tư **AF\_INET** nhưng dùng với Ipv6
* **socket\_type**: Đại diện cho loại socket và có thể là SOCK\_STREAM hoặc SOCK\_DGRAM.
  + **SOCK\_DRAM**: Đảm bảo kết nốt một chiều
  + **SOCK\_STREAM:** Đảm bảo kết nối dữ liệu 2 chiều
* **protocol**: Đây là một đối số tùy chọn, và nó thường mặc định là 0.
  + IPPROTO\_RAW: Ở đây để có thể sử dụng gói tin thô do người dùng tạo ra chúng ta cần sử dụng giao thức IPPROTO\_RAW.



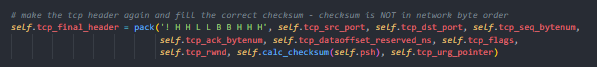
1. Các bước xây dựng socket truyền vector tấn công



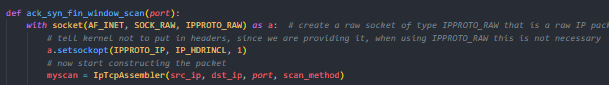
* Bước 1: Xây dựng các trường dữ liệu của gói tin.



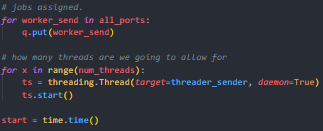
* Bước 2: Pack các trường dữ liệu thành các bit để gửi đi



* Bước 3: Khởi tạo socket gửi và nhúng gói tin vào socket

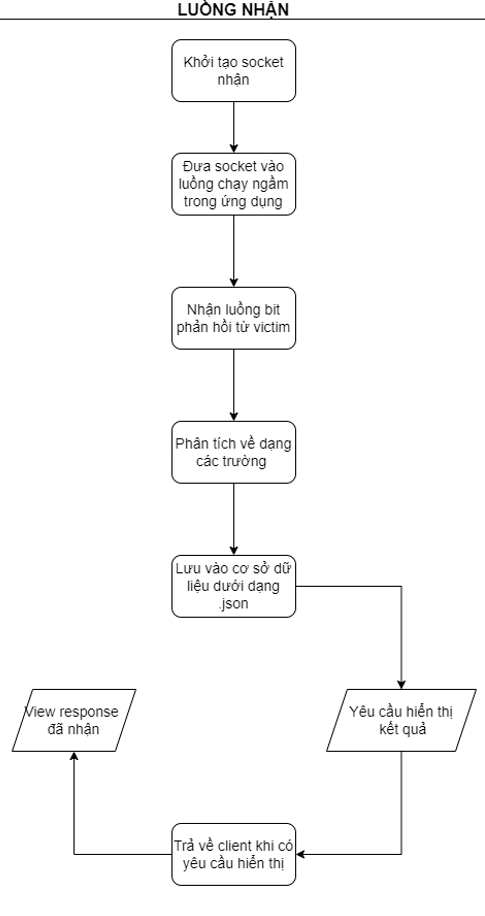


* Bước 4: Đưa socket vào đa luồng nhằm optimize tốc độ kiểm thử

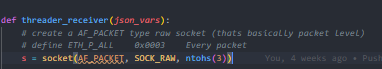


* Bước 5: Gửi gói tin

1. Các bước xây dựng socket nhận gói tin phản hồi

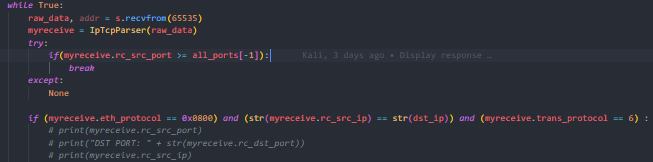


* Bước 1: Khởi tạo socket nhận và dump vào ứng dụng.

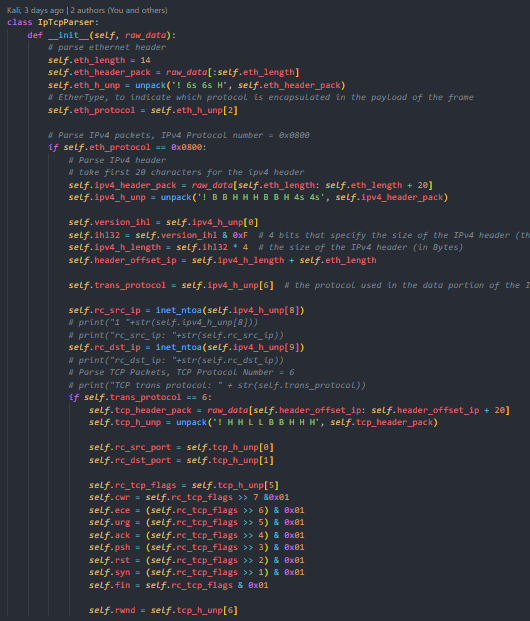




* Bước 2: Nhận luồng và xử lý bit phản hồi từ victim



* Bước 3: Phân tích về dạng các trường dữ liệu.



* Bước 4: Trả về dạng .json

