\*Tháng đầu tiên: ((\_\_/\_\_\_ – \_\_\_/\_\_\_)

- Mục tiêu chính: Hoàn thành thuật toán nhận diện sử dụng.

- Tuần đầu tiên + thứ hai(\_\_/\_\_\_ – \_\_\_/\_\_\_): Tìm kiếm, thử nghiệm code chạy được và xác định mô hình sử dụng trong thuật toán. Đi sâu vào nghiên cứu thuật toán, câu lệnh, tham số,… Nắm vững code như code của mình.

- Tuần thứ ba((\_\_/\_\_\_ – \_\_\_/\_\_\_): Viết bản thống kê sơ lược thuật toán, đặc điểm mô hình, các tham số và kỹ thuật xử lý được sử dụng trong code. Tiến hành hoàn thiện code, thay đổi, thử nghiệm, đánh giá, so sánh với các mô hình khác. Chụp lại kết quả thực nghiệm cho các lần thực nghiệm trên bộ dữ liệu.

\*Tháng thứ hai + nửa tháng thứ 3 ((\_\_/\_\_\_ – \_\_\_/\_\_\_): Tiến hành tìm hiểu và xây dựng mô hình đưa ra thực nghiệm   
- Mục tiêu chính: Xây dựng được hệ thống Server-Client cỡ nhỏ, có thể bắt gói tin và thu thập số liệu đựa trên mẫu data sử dụng huấn luyện. Đưa được thuật toán vào phần chính nhận diện và xử lý. Liên kết được hoàn toàn giữa hệ thống – model nhận diện – tường lửa – quản lý gói tin – quản lý user – phân phối tài nguyên.

- Tuần đầu tiên((\_\_/\_\_\_ – \_\_\_/\_\_\_): Tìm hiểu và triển khai các thiết bị router, switch, các máy chủ phân tán có khả năng điều hướng và bắt được gói tin đồng thời trích xuất được thông tin cần thiết. Triển khai hệ thống Server phân tán có triển khai model nhận diện và xử lý.

- Tuần thứ hai + ba((\_\_/\_\_\_ – \_\_\_/\_\_\_): Đồng thời triển khai hệ thống tường lửa xử lý vấn đề khi model nhận diện được các cuộc tấn công. liên kết hệ thống nhận diện với các router để có thể điều hướng hoặc xử lý khi có tấn công DoS/DdoS.

- Tuần thứ tư((\_\_/\_\_\_ – \_\_\_/\_\_\_): Triển khai IDS liên kết với các phần quản lý port và quản lý các gói tin. triển khai IDS truy vết gói tin và xử lý khi bị tấn công U2R hoặc trojan.

- Tuần thứ năm + sáu + bảy((\_\_/\_\_\_ – \_\_\_/\_\_\_): Tiến hành chỉnh sửa, đưa các model vào hệ thống đã hoàn thiện. Tiến hành thử nghiệm tấn công lấy ra các hình ảnh và số liệu thực nghiệm.