**TỔNG HỢP NHỮNG NỘI DUNG CHÍNH VỀ NCKH**

// Do mới được tiếp cận nên vẫn chưa có nhiều kiến thức để đưa ra biện pháp cho việc cải thiện được khả năng phát hiện xâm nhập, nhưng sau khi tìm hiểu sơ lược qua thì việc chúng ta ứng dụng GNN để phát hiện các bất thường và dự đoán rủi ro an ninh mạng có lẽ sẽ phát hiện được các lỗ hổng hoặc hành vi tấn công trong hệ thống phần mềm.

**TỔNG QUAN VỀ NGHIÊN CỨU**

* Đặc điểm của dữ liệu đồ thị: hệ thống có thể được biểu diễn dưới dạng đồ thị, với:
* Nút (node) biểu diễn các thực thể: tiến trình, gói tin, hàm trong mã nguồn, hoặc tài nguyên hệ thống.
* Cạnh (edge) biểu diễn các mối quan hệ: kết nối mạng, lời gọi hàm, hoặc sự phụ thuộc dữ liệu.

- Ứng dụng GNN trong an ninh mạng:

1. Phát hiện bất thường (anomaly detection) trong lưu lượng mạng.
2. Phân loại mã độc dựa trên biểu diễn đồ thị của chương trình.
3. Dự đoán lỗ hổng bảo mật dựa trên quan hệ giữa các hàm/module trong code base.

**//Comment: vẫn đang tìm hiểu thêm**

**…**

* **NHỮNG HƯỚNG PHÁT TRIỂN TA CÓ THỂ TÌM HIỂU TỚI**
* Kết hợp GNN với phương pháp lượng tử (Quantum Machine Learning) để tận dụng khả năng xử lý song song và mở rộng cho đồ thị cực lớn.
* Phát triển cơ chế giải thích mô hình (Explainable GNN) giúp chuyên gia an ninh hiểu rõ lý do dự đoán.