



Phạm Anh Tuấn

Thông tin cá nhân

- Ngày sinh:** 22/07/2004
- Số điện thoại:** +84 943326373
- Email:** 080at080@gmail.com
- LinkedIn:** https://www.linkedin.com/in/pham-anh-tuan-148b9b1a3/
- Địa chỉ:** Văn Canh, Hoài Đức, Hà Nội

Mục tiêu nghề nghiệp

Sinh viên năm cuối chuyên ngành Công nghệ thông tin ứng dụng, Đại học Quốc gia Hà Nội. Với nền tảng kiến thức về **An toàn thông tin, Quản trị cơ sở dữ liệu và Linux**, em mong muốn có cơ hội để trở thành **thực tập sinh/Fresher An ninh mạng (Security Analyst/Pentester)**.

Mục tiêu của em là áp dụng tư duy phòng thủ chiêu sâu (**Defense in Depth**) học được từ ghế nhà trường vào thực tế doanh nghiệp, đồng thời rèn luyện kỹ năng xử lý sự cố và đánh giá lỗ hổng bảo mật.

Cam kết thái độ làm việc kỷ luật, cầu thị và gắn bó lâu dài.

Kỹ năng

- OS:** Linux (Ubuntu, Kali), Windows Server.
- Network:** Wireshark, TCP/IP, VPN.
- Tools:** Burp Suite, Metasploit, Docker.
- Database:** PostgreSQL, MySQL, MinIO.
- Coding:** Python (Scripting), Bash Shell.

Chứng chỉ

Học vấn

Trường Quốc tế - Đại học Quốc gia Hà Nội (VNU-IS)

Công nghệ thông tin ứng dụng (Applied IT)

2022 - 2026

GPA : 2.9

Tham gia tích cực hoạt động trường

Tham gia NCKH

Kinh nghiệm làm việc

Dự án thực tế

Giải pháp Backup & Recovery chống Ransomware cho Database

Thực hiện đề tài

2024 - 2025

Mô tả: Xây dựng quy trình sao lưu dữ liệu tự động cho PostgreSQL, đảm bảo khả năng phục hồi khi hệ thống bị tấn công mã hóa dữ liệu.

Công việc thực hiện:

- Triển khai quy tắc backup **3-2-1** (3 bản sao, 2 định dạng, 1 bản offsite).
- Cấu hình tính năng **Object Locking** (WORM - Write Once Read Many) trên MinIO để ngăn chặn Hacker sửa/xóa file backup.
- Viết kịch bản (Script) phục hồi dữ liệu tự động (Disaster Recovery).

Kết quả: Hệ thống backup hoạt động ổn định, dữ liệu được bảo vệ toàn vẹn trước kịch bản tấn công giả lập.

Nghiên cứu Tấn công & Phòng thủ Prompt Injection trên LLM

Thực hiện đề tài

2025 - 2026

Mô tả: Nghiên cứu các phương thức tấn công vào mô hình ngôn ngữ lớn (Large Language Models - LLMs) tiếng Việt nhằm vượt qua các lớp bảo mật (Guardrails).

Công việc thực hiện:

- Xây dựng tập dữ liệu (Dataset) các câu lệnh độc hại (Malicious Prompts) đặc thù cho ngôn ngữ Tiếng Việt.
- Thực nghiệm các kỹ thuật **Jailbreak** (như DAN, Developer Mode) để đánh giá mức độ an toàn của các mô hình LLM phổ biến.
- Nghiên cứu tinh chỉnh (Fine-tune) mô hình cục bộ (Local Model) để giả lập kịch bản tấn công tự động.

PortSwigger Web Security
Academy - In progress

Sở thích

Mày mò nghiên cứu
Thể thao (Gym & Bóng rổ, Bóng đá):

Danh hiệu và giải thưởng