



## KỸ SƯ AN TOÀN THÔNG TIN

ĐẶNG LINH HẠNH

### MỤC TIÊU NGHỀ NGHIỆP

Tôi kỳ vọng được phát triển kỹ năng lập trình bảo mật với Python hoặc Bash, phục vụ cho việc xây dựng script tự động hóa kiểm tra bảo mật, phân tích log và xử lý sự cố theo thời gian thực.

### THÔNG TIN CÁ NHÂN

14/04/1981

Hà Nội

thaolinh252512@gmail.com

0307048260

www.website.com

### HỌC VẤN

- Quản trị và bảo mật hệ thống mạng  
tại Đại học CNTT - ĐHQG TP.HCM -  
Công nghệ thông tin tại Đại học Công  
nghệ - ĐHQG Hà Nội

### KỸ NĂNG

- Wireshark

### SỞ THÍCH

### KINH NGHIỆM LÀM VIỆC

- **CLOUD SECURITY ENGINEER** TẠI CLOUDGUARD ASIA  
(2021-2023)

+ THIẾT LẬP CHÍNH SÁCH IAM VÀ MÃ HÓA DỮ LIỆU  
TRONG AWS

+ KIỂM SOÁT TRUY CẬP S3, CLOUDTRAIL VÀ QUẢN LÝ  
CLOUDWATCH ALERT

+ PHÁT HIỆN CẤU HÌNH SAI BẰNG AWS CONFIG VÀ  
VIẾT LAMBDA XỬ LÝ TỰ ĐỘNG

- **CYBERSECURITY SPECIALIST** TẠI FINSEC VIỆT NAM  
(2020-2022)

- Du lịch

## NGƯỜI GIỚI THIỆU

- Bà Nguyễn Ngọc Ánh (Senior Security Engineer – BizSecure) -  
anh.nguyen@bizsecure.vn - 0966888777

+ ĐÁNH GIÁ LỖ HỔNG ĐỊNH KỲ BẰNG NESSUS VÀ VIẾT  
BÁO CÁO KHUYẾN NGHỊ

+ KIỂM THỬ BẢO MẬT ỨNG DỤNG WEB NỘI BỘ THEO  
TIÊU CHUẨN OWASP TOP 10

+ TRIỂN KHAI XÁC THỰC HAI YẾU TỐ (2FA) CHO HỆ  
THỐNG ERP VÀ EMAIL

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm  
trọng trong hệ thống email

- **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn  
kế hoạch 2 tuần

## CHỨNG CHỈ

- **2022** - Certified Information Systems Security Professional  
(CISSP) – ISC<sup>2</sup>

- **2023** - CompTIA PenTest+ – CompTIA

## HOẠT ĐỘNG

- **Diễn giả khách mời tại Hội thảo 'CyberSec Career Day'  
(2023)**

+ Trình bày lộ trình nghề nghiệp dành cho kỹ sư An toàn  
Thông tin.

+ Chia sẻ kinh nghiệm thực tế về triển khai hệ thống SIEM.

+ Tư vấn sinh viên về định hướng chuyên sâu Red Team và Blue Team.

## DỰ ÁN

### - Tự động hóa kiểm tra cấu hình bảo mật hệ thống (DevSecOps Engineer, DevShield) 2021

Xây dựng công cụ nội bộ dùng Python và Bash để kiểm tra định kỳ các cấu hình sai lệch và gửi báo cáo cho quản lý.

- + Phân tích các tiêu chuẩn cấu hình an toàn cho Linux server
- + Viết script kiểm tra các thiết lập quan trọng (sudo, ssh, firewall)
- + Gửi báo cáo HTML qua email mỗi tuần tự động

### - Đánh giá bảo mật ứng dụng web nội bộ (Pentester, SecureCode Labs) 2021

Thực hiện kiểm thử xâm nhập cho các ứng dụng web nội bộ nhằm xác định và khắc phục lỗ hổng OWASP Top 10.

- + Sử dụng Burp Suite, Nikto, OWASP ZAP để phân tích lỗ hổng
- + Viết báo cáo phân tích và hướng dẫn khắc phục chi tiết
- + Hỗ trợ đội phát triển sửa lỗi và tái kiểm tra

### - Triển khai hệ thống phát hiện xâm nhập mạng nội bộ (IDS) (Security Engineer, CyberDefense Việt Nam) 2022

Xây dựng hệ thống Snort IDS để giám sát và cảnh báo các mối đe dọa trong mạng nội bộ của doanh nghiệp.

- + Cài đặt và cấu hình Snort trên server Ubuntu
- + Tích hợp Snort với hệ thống cảnh báo nội bộ qua email
- + Huấn luyện đội vận hành đọc log và phản hồi sự cố

**- Xây dựng hệ thống SIEM nội bộ (Security Analyst, FinSec Việt Nam) 2022**

Tập hợp log từ các hệ thống và phân tích cảnh báo an ninh bằng ELK Stack (Elasticsearch, Logstash, Kibana).

+ Cấu hình Logstash để thu thập log từ firewall, server, IDS

+ Tạo dashboard trong Kibana theo dõi bất thường

+ Viết quy tắc cảnh báo và quy trình xử lý sự cố