



## KỸ SƯ AN TOÀN THÔNG TIN

NGUYỄN KHÁNH DŨNG

### MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn nghiên cứu và triển khai các cơ chế bảo mật nâng cao như Zero Trust, Network Segmentation, và bảo vệ dữ liệu trong môi trường hybrid cloud.

### THÔNG TIN CÁ NHÂN

13/02/2000

Hà Nội

thaolinh252512@gmail.com

0827561772

www.website.com

### HỌC VẤN

- Mạng máy tính và truyền thông dữ liệu tại Đại học Giao thông Vận tải

### KỸ NĂNG

- OWASP Top 10

### SỞ THÍCH

- Nghe nhạc

### KINH NGHIỆM LÀM VIỆC

- **SECURITY ANALYST** TẠI CYBERDEFENSE VIỆT NAM (2020-2021)

+ GIÁM SÁT HỆ THỐNG IDS/IPS SNORT VÀ XỬ LÝ CẢNH BÁO

+ XÂY DỰNG QUY TRÌNH PHẢN HỒI SỰ CỐ THEO CHUẨN NIST

+ PHỐI HỢP BỘ PHẬN PHÁT TRIỂN ỨNG DỤNG TÍCH HỢP SAST/DAST VÀO CI/CD

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

- Tham gia hackathon

- Trồng cây

- Đọc sách

## NGƯỜI GIỚI THIỆU

- Ông Trịnh Văn Kiên (Pentest Team Lead – SecureTest Lab) -  
kien.trinh@securetest.vn - 0944222333

- Ông Trần Quang Minh (Security Operations Manager – FinSec Việt Nam) -  
minh.tran@finsec.vn - 0933666888

- Bà Trần Kim Ngân (Security Compliance Officer – DevSecure) -  
ngan.tran@devsecure.vn - 0933444555

- Bà Lương Thị Thanh (Incident Response Manager – SafeNet) -  
thanh.luong@safenet.vn - 0977333555

+ 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)

+ 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

- **PENETRATION TESTER** TẠI SECURECODE LABS (2019-2021)

+ THỰC HIỆN KIỂM THỬ XÂM NHẬP MẠNG NỘI BỘ VÀ ỨNG DỤNG WEB

+ VIẾT SCRIPT TỰ ĐỘNG HÓA KHAI THÁC LỖ HỔNG CƠ BẢN VỚI PYTHON

+ TƯ VẤN CẢI TIẾN CẤU HÌNH BẢO MẬT HỆ THỐNG CHO KHÁCH HÀNG DOANH NGHIỆP

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn kế hoạch 2 tuần
- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng
- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email
- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức
- **2020** - Top 5 kỹ sư có phản ứng sự cố nhanh nhất trong hệ thống nội bộ

## CHỨNG CHỈ

- **2020** - Certified Ethical Hacker (CEH) – EC-Council

## HOẠT ĐỘNG

- Người viết blog bảo mật thông tin tại [infosecjournal.vn](https://infosecjournal.vn) (2021 - nay)

+ Chia sẻ kiến thức về bảo mật hệ thống và ứng dụng web.

+ Hướng dẫn kiểm tra bảo mật với Kali Linux và Metasploit.

- + Viết phân tích kỹ thuật về các cuộc tấn công thực tế.

#### **- Thành viên diễn tập Red Team nội bộ tại Ngân hàng Tài chính Việt (2022)**

- + Thực hiện khai thác giả lập các lỗ hổng hệ thống nội bộ.

- + Viết script tự động hóa kiểm tra cấu hình sai trên firewall và IDS.

- + Lập kế hoạch và báo cáo lỗ hổng gửi nhóm Blue Team xử lý.

#### **- Tình nguyện viên hỗ trợ khóa học CEH tại CyberSecurity Training Center (2023)**

- + Chuẩn bị máy ảo tấn công và phòng thủ trong lab CEH.

- + Hỗ trợ học viên trong các bài thực hành hands-on.

- + Giải đáp thắc mắc về công cụ nmap, wireshark, metasploit.

#### **- Thực tập sinh kiểm thử bảo mật tại Công ty SecureTech (2020)**

- + Thực hiện quét lỗ hổng hệ thống nội bộ bằng Burp Suite và OWASP ZAP.

- + Hỗ trợ viết báo cáo lỗ hổng và đề xuất giải pháp khắc phục.

- + Tham gia đánh giá bảo mật website khách hàng theo OWASP Top 10.

## **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

#### **- Bảo mật hệ thống cloud AWS (Cloud Security Engineer, CloudGuard Asia) 2023**

Đánh giá và cải thiện bảo mật cho hệ thống web triển khai trên hạ tầng AWS.

- + Thiết lập IAM theo nguyên tắc phân quyền tối thiểu
- + Kích hoạt CloudTrail và cảnh báo hoạt động bất thường
- + Kiểm tra cấu hình S3 bucket, RDS và các dịch vụ công khai

#### **- 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

