



## KỸ SƯ AN TOÀN THÔNG TIN

BÙI DŨNG HẠNH

### 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

10/01/1984

Hà Nội

thaolinh252512@gmail.com

0726788851

www.website.com

### HỌC VẤN

- An toàn thông tin tại Học viện Kỹ thuật Mật mã

### KỸ NĂNG

- Wireshark
- Cloud Security (AWS, Azure)
- Linux Security
- SIEM (Splunk, ELK)
- Bash Scripting

### KINH NGHIỆM LÀM VIỆC

- **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

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

## SỞ THÍCH

- Chụp ảnh
- Nấu ăn
- Xem phim khoa học viễn tưởng
- Tham gia cộng đồng lập trình
- Thể thao

+ 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

## NGƯỜI GIỚI THIỆU

- Bà Phạm Thị Mai (Cybersecurity Lead - TechShield) - mai.pham@techshield.vn - 0988999666

- **SECURITY ENGINEER** TẠI CÔNG TY ANTOANTECH (2021-2023)

+ TRIỂN KHAI VÀ GIÁM SÁT HỆ THỐNG SIEM (ELK STACK) ĐỂ PHÁT HIỆN HÀNH VI BẤT THƯỜNG

+ CẤU HÌNH TƯỜNG LỬA NỘI BỘ VÀ VPN BẢO VỆ TRUY CẬP TỪ XA

+ PHÂN TÍCH LOG HỆ THỐNG, ĐIỀU TRA SỰ CỐ BẢO MẬT VÀ ĐƯA RA BIỆN PHÁP XỬ LÝ

- **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

## DANH HIỆU VÀ GIẢI THƯỞNG

- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống cảnh báo an ninh mạng
- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức

## CHỨNG CHỈ

- **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals
- **2021** - Cisco Certified CyberOps Associate - Cisco
- **2023** - CompTIA PenTest+ - CompTIA
- **2022** - Certified Information Systems Security Professional (CISSP) - ISC<sup>2</sup>
- **2021** - CompTIA Security+ - CompTIA

## HOẠT ĐỘNG

- **Người viết blog bảo mật thông tin tại 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 nhóm nghiên cứu bảo mật tại Phòng Lab An toàn Thông tin - Đại học Bách khoa (2021 - 2023)**

- + Nghiên cứu về các lỗ hổng bảo mật phổ biến như XSS, SQLi, CSRF.

- + Tham gia diễn tập phát hiện và ứng phó sự cố tấn công mạng.

- + Viết báo cáo kỹ thuật và trình bày tại hội nghị sinh viên NCKH.

## 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

**- 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

## **- 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

