



KỸ SƯ AN TOÀN THÔNG TIN

VŨ QUỲNH NAM

MỤC TIÊU NGHỀ NGHIỆP

Tôi đặt mục tiêu học và ứng dụng các phương pháp bảo mật hệ thống mạng như IDS/IPS, VLAN, Firewall rules, VPN để phòng ngừa và ngăn chặn các cuộc tấn công có chủ đích vào hạ tầng CNTT.

THÔNG TIN CÁ NHÂN

02/11/1995

Hà Nội

thaolinh252512@gmail.com

0941563849

www.website.com

HỌC VẤN

- Khoa học máy tính tại Đại học Quốc tế - ĐHQG TP.HCM

KỸ NĂNG

- Web Application Security
- Incident Response
- Zero Trust Architecture
- Burp Suite
- Bash Scripting

KINH NGHIỆM LÀM VIỆC

- **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

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

SỞ THÍCH

- Thử nghiệm công nghệ mới
- Tham gia cộng đồng lập trình
- Chơi đàn guitar

NGƯỜI GIỚI THIỆU

- Ông Đỗ Minh Tiến (Head of Cloud Security – CloudBase VN) - tien.do@cloudbase.vn - 0911555666
- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999

+ 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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật
- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống cảnh báo an ninh mạng
- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng
- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức
- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm trọng trong hệ thống email

CHỨNG CHỈ

- **2023** - AWS Certified Security – Specialty
- **2023** - CompTIA PenTest+ – CompTIA
- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²

- **2021** - CompTIA Security+ - CompTIA

HOẠT ĐỘNG

- **Thành viên câu lạc bộ An toàn thông tin tại CLB Sinh viên An ninh mạng - Học viện Kỹ thuật Mật mã (2020 - 2022)**

+ Tổ chức các buổi workshop về bảo mật Wi-Fi, DNS spoofing.

+ Tham gia thi đấu CTF nội bộ và luyện tập giải bài reversing.

+ Chia sẻ tài liệu và tổng hợp hướng dẫn học về pentest.

- **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.

- **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.

DỰ ÁN

- **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

- 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

- 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

