KỸ SƯ AN TOÀN THÔNG TIN

TRẦN HÀ LAN

MỤC TIÊU NGHỀ NGHIỆP

Tôi hướng đến xây dựng các công cụ nội bộ giúp kiểm tra cấu hình bảo mật định kỳ, tự động hóa việc đánh giá lỗ hổng hệ thống và gửi báo cáo hàng tuần cho quản lý.

THÔNG TIN CÁ NHÂN

16/06/1986
Hà Nội
thaolinh252512@gmail.com
0934692093
www.website.com

HỌC VẤN

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

KỸ NĂNG

- OWASP Top 10

SỞ THÍCH

- Tham gia hội thảo công nghệ

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

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

- Học ngoại ngữ

- Xem phim khoa học viễn tưởng

- Du lịch

NGƯỜI GIỚI THIỆU

- Ông Đỗ Minh Tiến (Head of Cloud Security – CloudBase VN) - tien.do@cloudbase.vn - 0911555666

- Ông Vũ Văn Duy (Quản lý hệ thống bảo mật – DataSafe Solutions) - duy.vu@datasafe.vn - 0909111222

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

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

+ 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** - Nhân viên An toàn Thông tin xuất sắc quý III tại Công ty AnToanTech

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật

- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức

- **2021** - Được đề cử danh hiệu 'Gương mặt trẻ lĩnh vực An ninh mạng'

CHỨNG CHỈ

- **2021** - Microsoft Certified: Security, Compliance, and Identity Fundamentals

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.

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

- 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

- 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

- 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