KỸ SƯ AN TOÀN THÔNG TIN

BÙI NGA ANH

MỤC TIÊU NGHỀ NGHIỆP

Tôi định hướng phát triển thành một Security Engineer có tư duy phản biện cao, sẵn sàng phát hiện bất thường từ log hệ thống, mã nguồn, hoặc hành vi người dùng để ngăn chặn nguy cơ bị khai thác.

THÔNG TIN CÁ NHÂN

08/04/1987
Hà Nội
thaolinh252512@gmail.com
0382987345
www.website.com

HỌC VẤN

- Quản trị và bảo mật hệ thống mạng tại Đại học CNTT – ĐHQG TP.HCM - Kỹ thuật phần mềm tại Đại học Bách khoa Hà Nội

KỸ NĂNG

- Security Compliance (ISO 27001, NIST, PCI-DSS)

- Incident Response

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

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

SỞ THÍCH

- Thể thao

- Tham gia hội thảo công nghệ

- Đi bộ đường dài

- Nấu ăn

- Viết blog kỹ thuật

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

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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

- **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

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

CHỨNG CHỈ

- **2022** - Offensive Security Certified Professional (OSCP)

- **2022** - Certified Information Systems Security Professional (CISSP) – ISC²

- **2021** - Cisco Certified CyberOps Associate – Cisco

- **2022** - Certified Cloud Security Professional (CCSP) – ISC²

HOẠT ĐỘNG

- Cộng tác viên chương trình đánh giá bảo mật hệ thống tại Công ty SafeNet (2021)

+ Kiểm tra cấu hình tường lửa, phân quyền tài khoản trên hệ thống.

+ Thực hiện quét port, phát hiện dịch vụ không an toàn.

+ Tổng hợp báo cáo lỗ hổng gửi khách hàng.

- Mentor nhóm sinh viên nghiên cứu bảo mật web tại CLB IT trẻ (2022)

+ Hướng dẫn khai thác lỗi XSS, CSRF trên các bài thực hành.

+ Giám sát và hỗ trợ quá trình viết báo cáo kỹ thuật.

+ Chấm điểm phần trình bày đề tài bảo mật cuối kỳ.

- Tình nguyện viên hỗ trợ sự kiện CTF tại Vietnam Cybersecurity Week (2022)

+ Hỗ trợ kỹ thuật cho các đội chơi trong cuộc thi Capture The Flag.

+ Cài đặt và cấu hình máy chủ hosting bài thi.

+ Giám sát an toàn hệ thống trong suốt thời gian diễn ra sự kiện.

- 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.

- 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

- 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

- 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