KỸ SƯ AN TOÀN THÔNG TIN

HOÀNG THU SƠN

MỤC TIÊU NGHỀ NGHIỆP

Tôi mong muốn trở thành cầu nối giữa đội ngũ DevOps và bảo mật (DevSecOps), giúp tích hợp quy trình bảo mật vào vòng đời phát triển phần mềm ngay từ giai đoạn đầu.

THÔNG TIN CÁ NHÂN

04/12/1991
Hà Nội
thaolinh252512@gmail.com
0846018832
www.website.com

HỌC VẤN

- An ninh mạng tại Đại học FPT - Khoa học máy tính tại Đại học Quốc tế – ĐHQG TP.HCM

KỸ NĂNG

- Incident Response
- Bash Scripting
- Python
- Cloud Security (AWS, Azure)
- Penetration Testing

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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống

SỞ THÍCH

- Nghe nhạc

- Thiết kế sản phẩm cá nhân

- Chơi đàn guitar

- Tham gia hackathon

- Đọc sách

NGƯỜI GIỚI THIỆU

- Bà Nguyễn Ngọc Ánh (Senior Security Engineer – BizSecure) - anh.nguyen@bizsecure.vn - 0966888777

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

cảnh báo an ninh mạng

- **2021** - Nhân viên An toàn Thông tin xuất sắc quý III tại Công ty AnToanTech

- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình bảo vệ dữ liệu khách hàng

- **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

- 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.

- 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.

- 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.

- 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.

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

- 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

- 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