KỸ SƯ AN TOÀN THÔNG TIN

PHẠM TÚ HẠNH

MỤC TIÊU NGHỀ NGHIỆP

Tôi đặt mục tiêu nâng cao kỹ năng kiểm thử xâm nhập (penetration testing), sử dụng các công cụ như Burp Suite, Metasploit, Kali Linux để đánh giá hệ thống và hỗ trợ phòng ngừa tấn công có chủ đích.

THÔNG TIN CÁ NHÂN

21/08/1992
Hà Nội
thaolinh252512@gmail.com
0781544686
www.website.com

HỌC VẤN

- Công nghệ thông tin tại Đại học Công nghệ – ĐHQG Hà Nội - Kỹ thuật an toàn thông tin tại Đại học Duy Tân

KỸ NĂNG

- Penetration Testing
- Python
- Network Security
- Identity and Access Management (IAM)

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

- Đọc sách

- Thiết kế sản phẩm cá nhân

- Trồng cây

- Nấu ăn

- Chơi cờ vua

NGƯỜI GIỚI THIỆU

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

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

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

- Ông Trịnh Văn Kiên (Pentest Team Lead – SecureTest Lab) - kien.trinh@securetest.vn - 0944222333

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

+ 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

- **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

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

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

- **2021** - Vinh danh cá nhân đóng góp nhiều nhất cho hệ thống cảnh báo an ninh mạng

CHỨNG CHỈ

- **2023** - AWS Certified Security – Specialty

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

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

HOẠT ĐỘNG

- 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.

- 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

- 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

- 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

- 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

- 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