KỸ SƯ AN TOÀN THÔNG TIN

BÙI HÀ LAN

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

22/04/1991
Hà Nội
thaolinh252512@gmail.com
0348690758
www.website.com

HỌC VẤN

- An ninh mạng tại Đại học FPT - Mạng máy tính và truyền thông dữ liệu tại Đại học Giao thông Vận tải

KỸ NĂNG

- IDS/IPS (Snort, Suricata)

SỞ THÍCH

- Tham gia cộng đồng lập trình

KINH NGHIỆM LÀM VIỆC

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2023** - Bằng khen vì hoàn thành kiểm thử xâm nhập sớm hơn

- Thể thao

- Trồng cây

- Học ngoại ngữ

NGƯỜI GIỚI THIỆU

- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999

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

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

- Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) - trung.nguyen@antoantech.vn - 0908666777

kế hoạch 2 tuần

- **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

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

- **2020** - Certified Ethical Hacker (CEH) – EC-Council

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

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

HOẠT ĐỘNG

- 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

- 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

- 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

- 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

- 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