KỸ SƯ AN TOÀN THÔNG TIN

ĐỖ THU HÀ

MỤC TIÊU NGHỀ NGHIỆP

Tôi đặt mục tiêu xây dựng một hệ thống honeypot để giám sát các hoạt động tấn công và phân tích hành vi kẻ tấn công nhằm cải thiện chính sách phòng thủ an ninh mạng.

THÔNG TIN CÁ NHÂN

26/07/1999
Hà Nội
thaolinh252512@gmail.com
0954805162
www.website.com

HỌC VẤN

- Mạng máy tính và truyền thông dữ liệu tại Đại học Giao thông Vận tải - Kỹ thuật an toàn thông tin tại Đại học Duy Tân

KỸ NĂNG

- Bash Scripting

SỞ THÍCH

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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2022** - Top 3 kỹ sư có đóng góp lớn nhất vào chương trình

- Trồng cây

- Viết blog kỹ thuật

- Tham gia hội thảo công nghệ

- Thiết kế sản phẩm cá nhân

NGƯỜI GIỚI THIỆU

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

- Bà Lương Thị Thanh (Incident Response Manager – SafeNet) - thanh.luong@safenet.vn - 0977333555

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

bảo vệ dữ liệu khách hàng

CHỨNG CHỈ

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

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

- **2020** - GIAC Security Essentials (GSEC) – SANS Institute

HOẠT ĐỘNG

- Người viết blog bảo mật thông tin tại infosecjournal.vn (2021 - nay)

+ Chia sẻ kiến thức về bảo mật hệ thống và ứng dụng web.

+ Hướng dẫn kiểm tra bảo mật với Kali Linux và Metasploit.

+ Viết phân tích kỹ thuật về các cuộc tấn công thực tế.

- 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.

- 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.

- 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.

- 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

- 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