KỸ SƯ AN TOÀN THÔNG TIN

ĐỖ HIẾU TÙNG

MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn góp phần xây dựng hệ thống Security Awareness Training trong doanh nghiệp, giúp nhân viên hiểu về các nguy cơ như phishing, malware và tăng cường ý thức bảo vệ tài sản số.

THÔNG TIN CÁ NHÂN

18/10/1997
Hà Nội
thaolinh252512@gmail.com
0398175979
www.website.com

HỌC VẤN

- Quản trị và bảo mật hệ thống mạng tại Đại học CNTT – ĐHQG TP.HCM - Công nghệ thông tin tại Đại học Công nghệ – ĐHQG Hà Nội

KỸ NĂNG

- Network Security

- Linux Security

- Vulnerability Assessment (Nessus, OpenVAS)

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

- **SECURITY ANALYST** TẠI CYBERDEFENSE VIỆT NAM (2020-2021)

SỞ THÍCH

- Chơi đàn guitar
- Xem phim khoa học viễn tưởng
- Du lịch
- Thử nghiệm công nghệ mới

+ 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

NGƯỜI GIỚI THIỆU

- 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
- Bà Lê Thị Huyền (Giám đốc An ninh Thông tin (CISO) – CloudSecure Corp) - huyen.le@cloudsecure.vn - 0912888999
- Ông Nguyễn Thành Trung (Trưởng phòng An toàn Thông tin – Công ty AnToanTech) - trung.nguyen@antoantech.vn - 0908666777

- **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)

+ 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

DANH HIỆU VÀ GIẢI THƯỞNG

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

- **2023** - Giải nhất cuộc thi 'Capture The Flag' toàn quốc do VietCyber tổ chức

CHỨNG CHỈ

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

HOẠT ĐỘNG

- Thành viên nhóm nghiên cứu bảo mật tại Phòng Lab An toàn Thông tin - Đại học Bách khoa (2021 - 2023)

+ Nghiên cứu về các lỗ hổng bảo mật phổ biến như XSS, SQLi, CSRF.

+ Tham gia diễn tập phát hiện và ứng phó sự cố tấn công mạng.

+ Viết báo cáo kỹ thuật và trình bày tại hội nghị sinh viên NCKH.

- 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.

- 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.

- 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