



KỸ SƯ AN TOÀN THÔNG TIN

ĐẶNG HÒA QUỲNH

MỤC TIÊU NGHỀ NGHIỆP

Tôi muốn trở thành chuyên gia trong việc phân tích và phản hồi sự cố bảo mật, từ việc thu thập log, phân tích forensics đến khôi phục hệ thống sau sự cố một cách nhanh chóng và hiệu quả.

THÔNG TIN CÁ NHÂN

20/07/1992

Hà Nội

thaolinh252512@gmail.com

0856550535

www.website.com

HỌC VẤN

- Khoa học máy tính tại Đại học Quốc
tế - ĐHQG TP.HCM

KỸ NĂNG

- OWASP Top 10
- Penetration Testing

SỞ THÍCH

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

- **CLOUD SECURITY ENGINEER** TẠI CLOUDGUARD ASIA
(2021-2023)

- Chụp ảnh

- Thử nghiệm công nghệ mới

NGƯỜI GIỚI THIỆU

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

- Ông Vũ Văn Duy (Quản lý hệ thống bảo mật - DataSafe Solutions) - duy.vu@datasafe.vn - 0909111222

+ 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 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

- **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

- **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

DANH HIỆU VÀ GIẢI THƯỞNG

- **2020** - Nhân viên triển khai SIEM hiệu quả nhất tại bộ phận bảo mật

- **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'

- **2022** - Giải thưởng 'Kỹ sư có sáng kiến bảo mật nội bộ' của năm

- **2022** - Bằng khen vì phát hiện sớm lỗ hổng bảo mật nghiêm

trọng trong hệ thống email

CHỨNG CHỈ

- **2021** - CompTIA Security+ – CompTIA
- **2020** - Certified Ethical Hacker (CEH) – EC-Council

HOẠT ĐỘNG

- 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.

- 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 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.

- 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.

DỰ ÁN

- 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

- 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

