letranquan2210@gmail.com

0343721932

facebook.com/Monterzi

175 Nguyễn Văn Tăng, phường Long Thạnh Mỹ, Quận 9, Tp. HCM

CÁ KỸ NĂNG

Tiếng Anh:

- Có khả năng đọc hiểu tài liệu.

Kỹ năng làm việc nhóm:

- Có kinh nghiệm làm việc nhóm trong các dự án phần mềm và kiểm thử thâm nhập.
- Sử dụng công cụ Git để quản lý phần mềm và các file code của dự án.
- Luôn có tinh thần hợp tác và giao tiếp tốt với các thành viên trong nhóm để đạt được mục tiêu của dự án.
- Có khả năng đưa ra ý kiến và giải pháp để giải quyết các vấn đề phát sinh trong quá trình làm việc nhóm.
- Có khả năng làm việc với các thành viên trong nhóm đến từ các văn hóa và lĩnh vực khác nhau, tôn trọng và hiểu được sự đa dạng của đội ngũ làm việc.

Kiến thức cơ bản về Mạng và System:

- Hiểu biết cơ bản về hệ thống máy tính và các hệ điều hành: Kali Linux, Ubuntu, EVE-NG, Security Onion, CentOS.
- Có kiến thức cơ bản cho cấu hình thiết bị mạng Cisco: Router, Switch.
- Cấu hình cơ bản của các giao thức mạng như TCP/IP, DHCP, NAT cũng như triển khai các tính năng bảo mật như firewall, IDS/IPS và VPN.
- Có kiến thức cơ bản về công cụ và phương pháp phân tích như Wireshark, tcpdump, ngrep, tshark và các kỹ thuật khác để phân tích lưu lượng mạng.

LÊ TRẦN MINH QUÂN

NETWORK ENGINEER INTERN

MỤC TIÊU NGHỀ NGHIỆP

Tôi mong muốn trở thành một Network Engineer Intern để phát triển kỹ năng CNTT, áp dụng kiến thức cơ bản về CNTT và mạng vào công việc thực tế, cùng đồng nghiệp hỗ trợ nhau trong làm việc nhóm. Tôi cũng hy vọng tham gia vào các dự án thực tế và học hỏi những kiến thức mới nhất trong lĩnh vực này

KINH NGHIỆM LÀM VIỆC

KIỂM THỬ THÂM NHẬP BẰNG WHITE BOX VÀ PENTESTING

// **04/2021 - 08/2021**

Xây dựng mô hình kết nối mạng theo chuẩn CCNA sử dụng EVE-NG và Cisco Packet Tracer

- Link github: *https://github.com/letranquan2210/Network-Connectivity*
- Số lượng thành viên: 1 (dự án cá nhân)
- Công nghệ sử dụng:
  - MS Windows host EVE-NGv2.5
  - Cisco Packet Tracer
- Chức năng chính:
  - Triển khai kết nối mạng với mô hình CCNA, bằng cách sử dụng các máy ảo trên MS Windows host EVE-NGv2.5. Sử dụng chương trình Cisco Packet Tracer để tạo và kết nối các mạng với nhau, đồng thời thiết lập và cấu hình các giao thức và thiết bị mạng tương ứng để đảm bảo hoạt động hiệu quả và ổn định của hệ thống.
  - Đã tìm hiểu và nắm được kiến thức cơ bản về mạng máy tính và các thiết bị mạng, bao gồm cấu trúc của các thiết bị, các giao thức mạng, các dịch vụ mạng cơ bản như DHCP, DNS, NAT, và ACL.
  - Đã làm việc trên Cisco Packet Tracer để xây dựng và thiết lập kết nối giữa các thiết bị mạng như Switch, Router, Firewall, Server.
  - Có kinh nghiệm cơ bản cho cấu hình các thiết bị mạng Cisco, đặc biệt là cấu hình VLAN, OSPF, BGP.
  - Đã học tập và áp dụng các chuẩn và quy trình của Cisco, bao gồm Cisco Networking Academy, CCNA R&S, CCNA Security, và CCNP Routing and Switching.
  - Có khả năng giải quyết các vấn đề và sửa chữa lỗi trong mạng máy tính, bao gồm tìm hiểu các thông tin debug, troubleshoot các lỗi thường gặp, và cải thiện hiệu suất mạng.
  - Cấu hình cho router, Firewall, giám sát lưu lượng mạng để đối phó các kiểu tấn công mạng như: DoS (DDoS), Virus, Malware, phòng thủ tấn công Handshaking, Tấn công từ phía trong và phía ngoài.

WHITE BOX TESTING AND PENTESTING REPORT // 11/2020 - 03/2021

Báo cáo kiểm thử thâm nhập bằng White Box và Pentesting cho hệ thống FSOFT

- Link github: *https://github.com/letranquan2210/Information-Assurance/tree/main/Ethical%20Hacking*
- Số lượng thành viên: 4 (dự án nhóm)
- Công nghệ sử dụng:

- Viết luật phòng thủ cho Snort và sử dụng được CentOS.

White hat hacker:

- Kinh nghiệm trong kiểm thử thâm nhập hệ thống thông tin bằng phương pháp White Box testing.
- Có kiến thức sử dụng các công cụ như NetDiscover, nmap, DIRP, wpscan, Wireshark và Snort để tìm kiếm các lỗ hổng bảo mật và mối đe dọa tiềm ẩn.
- Có kinh nghiệm thực hành và giải quyết các bài lab trên HackTheBox, VulnHub, HACKXOR,.v.vvv... những nền tảng website cung cấp các thử thách bảo mật đa dạng để phát triển kỹ năng tấn công và phòng thủ.

    - Kali Linux
    - Wireshark
    - Snort
    - Virtual Machine: VMware
- Chức năng chính:
    - Quản lý rủi ro: có khả năng xác định, đánh giá và giảm thiểu các rủi ro bảo mật trong hệ thống thông tin.
    - Kiểm thử thâm nhập: có kinh nghiệm trong kiểm thử thâm nhập hệ thống thông tin bằng các phương pháp White Box testing, sử dụng các công cụ như NetDiscover, nmap, DIRP, wpscan, Wireshark và Snort để tìm kiếm các lỗ hổng bảo mật và mối đe dọa tiềm ẩn.
    - Viết báo cáo: viết báo cáo chi tiết về các mối đe dọa / lỗ hổng tìm thấy trong quá trình kiểm thử thâm nhập, cung cấp các giải pháp khắc phục và mô tả các thủ tục và lịch trình để hoàn thành. Link báo cáo: https://github.com/letranquan2210/Information-Assurance/blob/main/Report%20SPM.pdf

KINH NGHIỆM VÀ KỸ NĂNG TRONG LĨNH VỰC AN NINH MẠNG VÀ QUẢN LÝ HỆ THỐNG

// **04/2020 - 10/2020**

Thực hiện việc viết rules phòng thủ cho Snort để giám sát và phát hiện các cuộc tấn công vào hệ thống mạng, đặc biệt là tấn công TCP Syn Flood và CVE-2020-0796.

- Link github: https://github.com/letranquan2210/Information-Assurance/blob/main/Network%20Forensics/Report-TCP-Syn-Flood-and-CVE-2020-0796.pdf
- Số lượng thành viên: 1 (dự án cá nhân)
- Công nghệ sử dụng:
    - CentOS
    - Wireshark
    - Snort
    - Virtual Machine: VMware
- Chức năng chính:
    - Phân tích các tấn công mạng để xác định nguyên nhân và tìm kiếm dấu vết của các hoạt động xấu.
    - Thu thập dấu vết tập tin khả nghi trong việc phân tích và giải mã các gói tin mạng để tìm ra các mối đe dọa tiềm ẩn.
    - Thực hiện cài đặt và cấu hình các máy chủ CentOS, quản lý hệ thống và giám sát tình trạng của các máy chủ đó.
    - Viết các rules cho Snort để phát hiện và ngăn chặn các tấn công mạng đối với hệ thống.
    - Phân tích các sự cố mạng để xác định nguyên nhân và đưa ra các giải pháp phù hợp.