Lê Trần Minh Quân

Phone: 0343721932
Email: letranquan2210@gmail.com
Address: Tp. Thủ Dầu Một, Tỉnh Bình Dương
Website: github.com/letranquan2210

OBJECTIVE

Systems analyst, system programmer or cybersecurity.

EDUCATION

Currently graduated from FPT university (Hanoi).
Courses taken include: Ethical Hacking and Offensive Security, Network Connetivity, Digital Forensics, Business Communication, Java Programing, Python programming.
Technical and frameworks: Kali Linux, CentOS Linux, Windows server, Security Onion, Git GUI, Git Bash, NetBean, Eclipse, Pycharm, Javascript, css, MySQL Server, Cisco packet tracer, EVE-NG, PuTTY, VMware, Word, Excel, Power Point.

WORK EXPERIENCE

Fresher Java, FPT SOFTWARE HOA LAC

Sep 2020 - Dec 2020

Backend web, build a Website by Java programing that can keep Car Park Management with CRUD. The program is used on PC withkeyboard and mouse activities. The object system include car park employees, operation administration, parking registration, booking office, check in/ check out of cars, car trip and parking lot.

PERSONAL PROJECT

Optimized Solutions For Web Application Scanners

Aug 2021 - Dec 2021

Project is web application crawlers and scanners, after that using tool in Kali Linux (Burp Suite) detecting vulnerabilities and securing the Web Application. Part of team designing and implementing, writting a system in Python (Selenium) to crawl source code website. Then, build a library written in Beautiful Soup (Python) where contain a lots prototype to check values and find login page (main idea of module crawler) include English and Vietnamese website.

Network-Connectivity with CCNA model

Apr 2021 - Aug 2021

Build a Network-connectivity with model CCNA. The program need a Virtual machines, that using MS Windows host EVE-NGv2.5. Using environment Cisco Packet Tracer program to build and draw link between networks connected.

White box testing and pentesting report: FSOFT Challenges

Jan 2021 - Mar 2021

The plans of the risk management mostly handle the risks and the vulnerability by identifying the risk, impacts, damages and provide generally appropriate solutions to minimize risks. White box testing that using some technical hacking to exploration (NetDiscover, nmap, DIRP, wpscan,detection and prevention of DDOS using Wireshark and Snort, etc...). Finally, write a pentesting report to show lists of threats/vulnerabilities, describing procedures and schedules for accomplishment.