NGUYEN NGOC TAI

[redacted]
[redacted]
https://www.linkedin.com/in/zauzooz/
https://github.com/zauzooz

EDUCATION

University of Information Technology 2024 - Present
Major: Information Security

LANGUAGES

English TOEIC LR 610

CERTIFICATES

CCNA https://ude.my/UC-18a9fbef-916c-4de7-90e8-2e45ce618e7c

SKILLS

Operation System	Ubuntu
Network Concept	OSI model, DNS, TCP/IP, DHCP, ...
Network Configuration	Switching (VLAN, STP), Routing (OSPF, BGP), Security (ACL, NAT), High Avaibility
Pentest-tools	Kali Linux, Metasploit, Nmap, Nessus, OpenVAS, MITRE ATT&CK framework.
Security Operation	Wireshark, Pfsense, Snort, Wazuh.
Security Standard	ISO 27001
Virtulization	VMWare
Scripting Languages	Bash, Powershell
Programming Language	Python, C++

PUBLICATIONS

An interpretable approach for trustworthy intrusion detection systems against evasion samples 04/2023 – 08/2023

DOI Link: https://doi.org/10.22144/ctujoisd.2023.030
Description: This is an academic research paper about the application of deep learning in the field of network intrusion detection system, published in the “CTU Journal of Innovation and Sustainable Development” and presented at Can Tho University.

EXPERIENCES

UIT Inseclab 09/2023 – 12/2023

Role: Researcher Intern
Team size: 3
Description: Conducting research on the application of multi-modal deep learning techniques to analyze encrypted network traffic for network traffic classification.

PROJECTS

Data Loss Prevention 09/2023 – 12/2023

Project Link: https://github.com/zauzooz/data-loss-prevention-solution
Team size: 4
Description: This is a project related to conducting analysis, risk assessment, redesigning network systems, and establishing policies for an enterprise network to ensure minimizing data loss by leveraging the ISO 27001 standards, network security and application security knowledges.
Role: Design a secure network model.
Tech Stack: ISO 27001.

Man-In-The-Middle Attack (MITM) via Phishing 09/2023 – 12/2023

Project Link: https://github.com/zauzooz/MITM_attacks_HTTP_HTTPS
Team size: 4
Description: This is a project related to conducting a phishing attack on an internal network system using the MITM (Man-in-the-Middle) attack method by conducting research on the MITRE ATT&CK framework.
Role: Develop malware and then perform phising attacks via emails.
Tech Stack: Kali Linux, C++, Powershell, mitmproxy, Active Directory, MITRE ATT&CK framework.

XDR: Wazuh 02/2023 – 05/2023

Team size: 4
Description: This is a project related to conducting research on Wazuh, an open-source XDR framework.
Role: Seting up experiment environment and then testing Wazuh features.
Tech Stack: Wazuh.

DDoS detection in Software Defined Network (SDN) 09/2022 – 12/2022

Github: https://github.com/zauzooz/NT101.N11.ANTT_Project
Team size: 4
Description: Building an application for SDN controler to against DDoS Attack.
Role: Building the network SDN topology and an application.
Tech Stack: Python, Ryu Controller, Containernet, Scapy.