

PHAN NGUYEN THI

SOC Tier 1

☎ 0967119671 | ✉ thipn.work@gmail.com | 🌐 st3ws | 📍 Vietnam

SKILLS

SECURITY OPERATIONS

Log & alert analysis (ELK),
Pass-The-Hash, lateral movement,
persistence mechanisms, Windows
Event IDs.

TOOLS / PLATFORMS

SIEM (Wazuh, ELK), K8s, Grafana,
Prometheus, Loki, Wireshark, FTK
Imager, Volatility, Autopsy, Burp Suite,
Sysmon.

SYSTEMS & NETWORKS

Active Directory, Windows Server, Linux
(Ubuntu, Debian, Kali), TCP/IP, ZFS,
Docker, pfSense.

PROGRAMMING

Python, Bash, PowerShell, SQL, C.

ENGLISH

- TOEIC 735
- Upper-Intermediate
- Proficient in all 4 skills (Listening, Speaking, Reading, Writing)

METHODOLOGIES

Scrum, Problem-solving, Technical
Documentation Translation.

EDUCATION

FPT UNIVERSITY DANANG

INFORMATION ASSURANCE

Graduated Dec. 2025 | DA NANG

Area of study: SOC

GPA: 7.5 (3.0)

CERTIFICATES

- **Cisco Ethical Hacker** – [Badge](#)
- **CCNA: Switching, Routing, and Wireless Essentials** – [Badge](#)
- **Jeopardy ASCIS2023** (Consolation Prize)

OBJECTIVE

Detail-oriented Cybersecurity professional specializing in Security Operations. Proven expertise in analyzing security logs, identifying complex attack vectors (such as lateral movement and Active Directory privilege escalation), and translating deep technical investigations into actionable intelligence. Seeking a SOC position to leverage hands-on experience with the ELK stack and malware analysis to actively strengthen organizational security posture.

WORK EXPERIENCE

CYBERSECURITY INTERN

Sep 2024 – Apr 2025

FPT Software Da Nang

- **Project:** Trained in PortSwigger and Burp Suite tools, enhancing practical skills in web application security. Gained a solid understanding of **ISO 27000** series standards, information security management, and risk assessment practices.
- **Role:** Conducted penetration testing on product websites to identify potential security risks or vulnerabilities. Compiled detailed reports on findings, providing actionable recommendations for mitigation and improvement to enhance the overall security posture.

PROJECTS

Wazuh SIEM & Threat Detection Lab

2026

Wazuh, pfSense, Sysmon, Suricata, VirusTotal

- Architected an isolated threat hunting environment utilizing pfSense to segment 5 VMs (Wazuh manager, attacker node, and Linux/Windows targets).
- Enhanced endpoint visibility by deploying Wazuh agents integrated with Sysmon, Suricata, and File Integrity Monitoring (FIM) for robust host and network intrusion detection.
- Automated threat intelligence lookups by integrating the VirusTotal API into Wazuh to enrich security alerts and detect malicious file hashes.

On-Premise DDoS Attack Detection using LLMs

2025

IoT, MQTT, Grafana

- **Role:** Designed and implemented a real-time observability dashboard (Grafana, Prometheus, Loki) to visualize critical MQTT broker metrics and system performance.
- Engineered a data collection pipeline to enable high-fidelity monitoring and incident detection for the backend system.

Github link: [Project Repository](#)

Database Forensics & Insider Breach Recovery

2026

Docker, ZFS, MySQL, Bash, n8n

- Developed automated log analysis logic and Bash-based attack simulation scripts to identify and respond to malicious SQL queries.
- Engineered an automated rollback mechanism and webhook-based alerting system (via n8n) for real-time incident mitigation.

Github link: [Project Repository](#)