Nguyen Truong Bao

Cybersecurity Intern | AI Security Intern | SOC Internship

Da Nang, Vietnam | bigzero3939@gmail.com | 0937 420 973 | truongbao.id.vn
linkedin.com/in/nguyen-truong-bao-347437250 | github.com/zewolkt3939

Summary

Cybersecurity student with hands-on experience in security monitoring, vulnerability assessment, web security testing, and network security. Experienced in building and operating security labs using Wazuh, Elastic Stack, Burp Suite, Nmap, Wireshark, Suricata, and Linux security tools. Completed hands-on cybersecurity labs through Hack The Box and PortSwigger Web Security Academy, with practical experience in log analysis, threat detection, vulnerability research, and security automation. Interested in SOC, Security Assessment, Penetration Testing, and emerging AI Security.

Education

Duy Tan University, B.Sc. in Cybersecurity – Da Nang, Vietnam
Expected Graduation: 09/2027

Experience

Automotive Cybersecurity Intern, LG Electronics R&D Vietnam (LG DUT Cyber Security Lab) July 2026 – Aug 2026

- Developed and validated Linux-based automotive cybersecurity solutions on webOS.
- Developed Python/Scapy tools for network packet generation and automated firewall validation.
- Conducted network security testing involving VLANs, unicast/multicast traffic, packet filtering, and traffic analysis.
- Analyzed network traffic using packet capture and Linux networking tools to validate security controls.

Cybersecurity Research Intern, Fore-Z Sept 2024 – Sept 2025

Tech Stack: WordPress, PHP, Burp Suite

- Reviewed WordPress plugin source code to identify security vulnerabilities.
- Performed manual vulnerability assessments and documented remediation reports.
- Investigated vulnerability impact and documented findings with reproduction steps and remediation recommendations.

Projects

AI-Powered Alert Prioritization Platform Aug 2025 – Dec 2025

Role: Backend & DevOps Engineer | GitHub

- Developed Python FastAPI services to automatically collect, normalize, and process security events from Wazuh Indexer for centralized analysis.
- Built an AI-assisted alert prioritization module that classifies security events such as SQL Injection, XSS, Brute Force, LFI, and DoS attacks, reducing manual triage workload.
- Implemented event correlation logic to identify multi-stage attack patterns by analyzing source IPs, destination assets, and attack timelines across multiple log sources.
- Integrated automated Telegram notifications for high-severity incidents, enabling real-time alert delivery to analysts and reducing response time.

Skills

Security Operations: Wazuh, Elastic Stack, Suricata, MITRE ATT&CK, Security Monitoring, Log Analysis, Threat Detection

Security Assessment: Burp Suite, Nmap, Nuclei, Nessus, Wireshark, Vulnerability Assessment, Web Security Testing

Network Security: TCP/IP, VLAN, Inter-VLAN Routing, ACL, NAT/PAT, STP, OSPF, DHCP, DNS, Network Segmentation

Systems & Programming: Linux, Python, SQL, Git

Security Engineering: iptables, ip6tables, nftables, Scapy, VMware, AWS

AI / Data: LLMs, Prompt Engineering, Pandas, NumPy

Certifications

- **Google Cybersecurity Professional Certificate** — Dec 2024

Cybersecurity Training & Labs

AI in Action — VinGroup, Cohort 4 | 12-week program – On-Going

- 6-week intensive training phase followed by a 6-week company/project placement phase.
- Developing practical skills in AI/LLMs and applied AI development.

Hack The Box

- Junior Cybersecurity Analyst Path — Completed Path
- Web Penetration Tester Path — 80%

PortSwigger Web Security Academy

- Completed 171 hands-on labs covering SQL Injection, Cross-Site Scripting (XSS), Authentication, Access Control, SSRF, File Upload, and other web vulnerabilities.

CyberDefenders

- Hands-on SOC/DFIR labs covering log analysis, threat detection, network traffic analysis, and incident investigation.

Languages

English: TOEIC 685 — Able to read technical documentation and communicate with teams.