

Phan Dinh Nhat

📍 Hanoi, Vietnam | @ contact@phannhat.id.vn | ☎ +84 96 259 77 80 | 🌐 phannhat.id.vn

🌐 linkedin.com/in/pdnhat | 🐙 github.com/phannhat17

Education

Hanoi University of Science and Technology, BS in Cyber Security Sept 2021 – Present

- GPA: 3.25/4.0
- **Coursework:** Computer Architecture, Network Defense, Malware Analysis, Digital Forensics

Experience

Cybersecurity Intern - Viettel Digital Talent Hanoi, July 2023 – Oct 2023

- One of the top 50 candidates with the best achievements.
- Researched NIST Cybersecurity Framework (CSF) and CIS Controls to improve security posture and align internal policies with industry standards.
- Assisted in policy development and collaborated with senior engineers to optimize security governance and compliance.

Information Security Engineer - Viettel IT Division Hanoi, Nov 2023 – Apr 2025

- Led compliance audits across the corporation to ensure adherence to security standards, policies, and regulatory frameworks.
- Assessed and enhanced incident response quality by reviewing and optimizing SOC ticket handling processes.
- Worked closely with SOC teams to evaluate and improve the effectiveness of security event monitoring and response workflows.

Achievements

ASEAN Student Contest on Information Security (ASCIS)

- 2023: Attack-Defense Phase - Third Prize (9th place overall)
- 2024: Attack-Defense Phase - Third Prize (4th place overall)

PwC Hack A Day CTF 2024 - Second Prize

Member of CTF Team [ph1sher](#)

- 2023: Rank 08 Vietnam
- 2024: Rank 29 Vietnam

Others international CTF tournaments

- 15th/315 in ISITDTU CTF 2024 Quals (Team)
- 43th/964 in n00bzCTF 2024 (Solo)
- 116th/2213 in DownUnderCTF 2023 (Solo)
- 8th/507 in SPACE HEROES 2023 (Team), etc.

Projects

Simple EDR System - Ongoing - [GitHub Repository](#)

- Designed and implemented a simple Endpoint Detection and Response (EDR) system, consisting of an EDR Agent and EDR Server.
- Developed an EDR Agent capable of collecting Windows Event Logs and detecting potential security threats.
- Built an EDR Server to aggregate logs from multiple endpoints, analyze suspicious activities, and enable

remote threat response.

- Gained hands-on experience in Windows logging mechanisms, security event monitoring, and EDR architecture.

Atomic RedTeam MITRE Coverage - [GitHub Repository](#)

- Developed a structured mapping of Atomic Red Team test cases to MITRE ATT&CK techniques, enabling enhanced security coverage assessment.
- Integrated SonarQube to analyze code quality, detect vulnerabilities.

Network Attack Detection - [GitHub Repository](#)

- Developed a system to detect network attacks using machine learning and anomaly detection techniques.
- Implemented RandomForest, Support Vector Machine (SVM), and AdaBoost to classify malicious and benign network activities.

Certificates

Google Cybersecurity Specialization - [Link](#)

NSE 1 Network Security Associate - [Link](#)

NSE 2 Network Security Associate - [Link](#)

Skills

Languages: Vietnamese, English (TOEIC 865)

Tools: Burpsuite, Nmap, Wireshark, Docker CLI, Sysmon, pwntools, etc.

Technical Knowledge: Web pentest, Security policy development, Networking, Docker, Scripting, Linux privilege escalation, etc.