Tung Thanh Nguyen

413-275-0693 | tung051024@gmail.com | linkedin.com/in/tung0510 | Portfolio

Education

University of Massachusetts Amherst — Amherst, MA

MS in Computer Science (Incoming Student) — *May 2027*

BS in Computer Science (GPA: 3.85/4) — *May 2026*

Coursework: Computer & Network Security, Reverse Engineering & Exploit Development, Digital Forensic, Applied Cryptography, Search Engine, Computer Systems, Computer Networks, Data Structures, Database Management

Technical Skills

Security Monitoring & Incident Response: SIEM (Splunk), Wireshark, Snort, Firewalls | *Threat Hunting, Anomaly Detection, Network Traffic Analysis, MITRE ATT&CK*

Pen-Testing & Vulnerability Management: Metasploit, Burp Suite, Nmap, OpenVAS | *Vulnerability Scanning, Exploitation, Web App Security*

Forensics & Malware Analysis: Autopsy, FTK Imager, Volatility, CyberChef, Capa, REMnux, FLARE VM | *Memory & Disk Forensics, Malware Reverse Engineering*

Cryptography: RSA, PKI, TLS, Symmetric/Asymmetric Encryption, Hashing, MAC

Programming & Systems: Python, C/C++, Linux (Bash), Windows, Flask, SQL, MQTT

Experience

IoT Cyber Defense Extern — Feb 2026 – Present

Extern, Inc. (Hydroficient)

- Conducting end-to-end IoT threat modeling on MQTT pipelines using STRIDE/CIA Triad, identifying **6** high-risk vulnerabilities in device-to-cloud communication.
- Implementing mutual TLS (mTLS) and PKI-based device authentication, eliminating spoofing and replay attack exposure across **10+** simulated edge devices.
- Developing Python-based monitoring tools for real-time anomaly detection and message integrity validation to strengthen zero-trust communication controls.

Software Developer Intern — June 2024 – Sep. 2024

IVS Individual System

- Developed an AI thunderstorm nowcasting model using TensorFlow on **20GB+** radar data, achieving **92%** accuracy and reducing runtime by **50%**.
- Built secure Flask backend APIs with robust validation, maintaining **98%** data integrity for **100+** internal users.

Projects

Metasploitable 2 Hardening & Exploitation Lab | *Greenbone/OpenVAS, Metasploit, CIS Benchmark*

- Executed end-to-end vulnerability management by scanning, validating, and exploiting OpenVAS findings, confirming **100%** of high-risk vulnerabilities.
- Mapped validated vulnerabilities to CIS Ubuntu Benchmark controls to prioritize remediation and align with security standards.
- Hardened system by removing insecure services and tightening auth to eliminate exploitable paths.

CVE-2019-18634 Analysis | *Course Project*

- Reproduced and analyzed CVE-2019-18634 via binary reverse engineering to examine buffer overflow exploitation paths; mapped attack vectors to MITRE ATT&CK framework.
- Produced a hardening checklist (Stack Canaries, ASLR, NX) and remediation guidance presented to faculty.

Backdoor Attacks in AI Models | *Research Paper*

- Analyzed backdoor attack techniques (e.g., Trojan Attacks, BadNets) in ML, highlighting risks in critical domains (automotive and healthcare).
- Proposed defenses and detection techniques (e.g., Dataset Sanitization) to improve model robustness.

Certifications & Programs

CompTIA Security+

Google Cybersecurity | *Coursera - Google*

Cybersecurity Mentorship | *MassCyberCenter*

Intermediate Cybersecurity | *CodePath*

Cyber Security 101 | *TryHackMe*