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

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

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*

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 security assessments using CIA Triad and STRIDE to identify vulnerabilities in MQTT-based pipelines.
- Mitigating MQTT risks via TLS encryption and PKI-based device identity to prevent spoofing and replay attacks.
- Developing Python monitoring tools to validate message integrity and support real-time anomaly detection.

Software Developer Intern — June 2024 – Sep. 2024

IVS Individual System

- Developed AI thunderstorm nowcasting model using TensorFlow on **20GB+** radar data, achieving **92%** accuracy and reducing runtime by **50%**.
- Engineered scalable data pipelines improving model precision while ensuring **98%** data integrity.
- Built a secure Flask backend and interactive web frontend used by **100+** internal users.
- Collaborated in Agile cross-functional teams to optimize performance and reliability.

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 all 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*

- Conducted binary reverse-engineering and vulnerability analysis of CVE-2019-18634; 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

Security+ | *CompTIA* (Pursuing)

Google Cybersecurity | *Coursera - Google*

Cybersecurity Mentorship | *MassCyberCenter*

Intermediate Cybersecurity | *CodePath*

Cyber Security 101 | *TryHackMe*