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, Fall 2026) *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 & Threat Detection: Autopsy, FTK Imager, Volatility, CyberChef, Capa, REMnux, FLARE VM | *Memory Forensics, Disk Analysis, Malware Reverse Engineering*

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

Penetration Testing: Metasploit, Burp Suite, Nmap, Hydra, Gobuster, John the Ripper | *Vulnerability Scanning, Password Cracking, Web App Security*

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

Programming & Systems: Python, C/C++, Linux, Windows, Bash

Experience

IVS Individual System June 2024 – Sep. 2024

Software Developer Intern - AI/ML Focused

- Developed AI thunderstorms nowcasting model with TensorFlow using radar data, achieving **92%** accuracy, reducing **50%** runtime.
- Engineered data pipelines to process **20GB+** of radar data, increasing model precision and scalability.
- Developed a secure Flask back end and interactive web front end, improving usability for **100+** internal users.
- Collaborated in cross-functional Agile teams to enhance model efficiency and ensuring **98%** data integrity.

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.

Cybersecurity Virtual Experience Programs | *Forage - AIG, Mastercard*

- Analyzed CISA vulnerability reports and drafted remediation strategies to strengthen enterprise security posture.
- Built a Python script simulating ransomware decryption brute-force to demonstrate incident response concepts.

Certificates

Security+ | *Comptia* (Pursuing)
Intermediate Cybersecurity | *CodePath*
Google Cybersecurity | *Google - Coursera*
Cyber Security 101 | *TryHackMe*