

# Tung Thanh Nguyen

413-275-0693 | [tung051024@gmail.com](mailto:tung051024@gmail.com) | [linkedin.com/in/tung0510](https://linkedin.com/in/tung0510) | [Portfolio](#)

## EDUCATION

### University of Massachusetts Amherst

BS in Computer Science

May 2026

GPA: 3.85/4

**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*

- Exploited and remediated vulnerable services (e.g., vsftpd, rlogin, PostgreSQL) to improve host security posture.
- Mapped findings to CIS Ubuntu Benchmark recommendations and implemented hardening: service removal, auth restrictions, and network lockdown.

### 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, Gradient Inspection) 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*