# Tony Lin

Cell: 803-448-4826 | tony.lin.professional@gmail.com | https://lintony6.github.io/Portfolio/

## Education

**University of South Carolina – Columbia, S.C.** **Anticipated Spring 2026**

- *Bachelor of Science in Computer Science, Concentration: Cybersecurity*

## Experience

**US ARMY RESERVE** **November 2022 – Present**

*Signal Operations Support Specialist*

- Led the establishment and operation of critical communication systems within Tactical Operations Centers (TOCs) to ensure seamless command and control during field deployments.
- Developed and delivered comprehensive training modules on TOC setup, equipment packing lists, and operational guides to significantly enhance overall team readiness.
- Instructed personnel on AN/PRC-148 (MBITR) and RT-1523 radio operation, utilizing hands-on methods to improve unit proficiency in critical communication protocols.
- Performed preventative and corrective maintenance on diverse communication devices and power generators, utilizing diagnostic tools to minimize system disruptions and ensure consistent operational readiness

**Life Cycle Engineering** **May 2025 – August 2025**

*Systems Administrator/Cybersecurity Professional*

- Architected and deployed virtualized security environments with VMware ESXi, then hardened Red Hat Linux and Windows Server VMs using DISA STIGs (RMF Steps 2 & 3) for penetration testing.
- Automated system hardening and configuration tasks with Ansible, ensuring consistent deployment of security baselines to meet NIST STIG and DoD compliance.
- Executed automated security assessments on RHEL systems, aligning with RMF Step 4, using SCAP Compliance Checker (SCC) and Nessus to identify Cat I, II, & III vulnerabilities and documenting findings in POA&Ms for remediation
- Supported RMF compliance (RMF Steps 4 & 6) by validating system hardening with STIG Viewer and continuously monitoring security posture through Splunk log analysis for threat detection and incident response.
- Developed and deployed diverse Capture-the-Flag (CTF) challenges in Docker containers, incorporating initial access, web application (XSS, IDOR, RCE), and specialized service vulnerabilities.
- Engineered advanced CTF scenarios featuring complex directory service (LDAP) and DNS vulnerabilities, challenging participants with credential extraction, privilege escalation, and unauthenticated zone transfers.
- Integrated various network service and misconfiguration vulnerabilities (e.g., FTP, SUDO, CUPS, SNMP, SMB) into CTF challenges to simulate real-world ethical hacking scenarios.

## Certifications & Clearance

- **DOD Security Clearance**: Secret
- **Certifications**: CompTIA Security+ CE, CompTIA Network+ CE, CompTIA Server+ CE