ANDREW VU

vut1907@my.uwstout.edu | LinkedIn Profile: www.linkedin.com/in/thanh-an-vu/ | Mobile: 715-440-8384

SUMMARY

Cybersecurity student with a strong practical mindset and hands-on experience in ethical web application exploitation, cloud computing, and secure service architecture, including penetration testing and threat modeling to protect digital assets. Driven to identify the human judgment, creativity, and critical thinking that complement rather than compete with AI-assisted security tools.

Github: github.com/thewanter

PROFESSIONAL CERTIFICATIONS

Certified Kubernetes Administrator (CKA) Aug 2026
Amazon Cloud Red Team Professional (ACRTP) – Pwned Labs Feb 2026
Amazon Web Services Certified Developer – Associate Feb 2026 – Feb 2029
Amazon Web Services Solutions Architect – Associate Jul 2025 – Jul 2028
Link: https://www.credly.com/users/anvu

HONORS AND AWARDS

- **Amazon Web Services Student Builder Group Leader (Nov 2025 – Nov 2026 | Gold Level):** First cloud club leader at UW–Stout, selected through a globally competitive program with a 13% acceptance rate.
- **fwd:cloudsec (2025):** Selected as one of eight recipients nationwide to receive a scholarship to attend the largest and most reputable cloud security conference in the United States
- **Cloud Village CTF: 6th** place at **BSidesSF & RSA (2026),** and **2nd** place at **RSA Conference (2025)**
- **Collegiate Cyber Defense League (CCDL)**: Achieved 1st place in Wisconsin and Top 5 Midwest Region (2025) in Collegiate Cyber Defense Competition (CCDC)

EXPERIENCES

Point North Network Inc *Inner Grove, MN, United States*
IT Security Intern June 2026 – Present

- Collaborated with Security Engineer to handle security alerts on Sentinel One, Datto RMM with 30+ corporate clients
- Co-authored security monitoring standards and baseline configuration documentation (M365, Active Directory, CIPP)
- Engineered security automation workflows in Rewst to streamline vulnerability remediation and alert triage, reducing manual overhead for the security team by automating patch-failure diagnostics in Datto RMM and clearing a backlog of automation requests using Python/PowerShell and DevOps practices

Maxcess International *Neenah, WI, United States*
IT Security Analyst Intern May 2025 – Sep 2025

- Collaborated with the Security Manager and global IT teams to secure enterprise environments with **2,000+** Active Directory devices
- Triaged and resolved **500+** security incidents using Arctic Wolf, including phishing, malware, and suspicious activities.
- Triaged vulnerabilities and performed asset analysis using Data Explorer and Axonius, collaborating with the Cisco Meraki firewall team to implement preventative security controls
- Introduced AI-assisted phishing detection workflows for encoded HTML and QR-code–based attacks missed by Proofpoint, reducing investigation time by **over 50%** and strengthening threat analysis

University of Wisconsin-Stout *Menomonie, WI, United States*
Computer Networking Teaching Assistant Aug 2024 – May 2025

- Guided **40+ students** on routing protocols, subnetting, and NAT, mapping them to AWS VPC, route tables, and security groups
- Introduced students to cryptography, access-control models, and security monitoring using AWS parallels
- Supported labs that reinforced translating on-premises networking into cloud security architectures

PROJECTS

Cloud, Web, AI Security Capture The Flag (CTF) Creator – UW-Stout

- Developed cloud computing and web, AI security for the semesterly competition; delivered a practical and comprehensive cloud security challenge focused on cloud infrastructure (Azure and AWS), including IAM role lateral movement, misconfigured role abuse, prompt injections, and red team techniques on a cloud-hosted platform

AWS IAM Privilege Escalation Mapper Cloud Security Project | github.com/thewanter/Threat_mapping

- Capstone project leader, led a team of 5. Built an IAM permission threat mapping tool leveraging *ListRoles* and *ListPolicies* to validate trust identities, automate *AssumeRole* checks, and reduce manual testing across organizations with numerous roles
- Enabled multi-account checks with filters for customer-managed roles and visualized results via an interactive Neo4j dashboard to improve visibility into IAM risks

EDUCATION

UNIVERSITY OF WISCONSIN - STOUT *Menomonie, WI, United States*
Bachelor of Cybersecurity (GPA: 3.9/4.0) Graduating: May 2027

SKILLS

- **Offensive Security Tools:** Kali Linux, Burp Suite, OWASP Top 10, Metasploit Framework, Wireshark
- **Programming & Cloud**: CI/CD, Kubernetes, Terraform, AWS (IAM, S3, EC2, CDK), Azure, Git, Python, Bash, Java, JavaScript