Chase Cooper

512-779-2142 | chasecooper393@gmail.com

Education

Sam Houston State University — Huntsville, TX

Bachelor of Science in Cyber Security; Minor in Computer Science - Information Systems — *Aug. 2024 – May 2027*

Experience

Junior SOC Analyst — Huntsville, TX

Sam Houston State University — *Fall 2025*

- Monitored and analyzed security alerts using Splunk to identify potential threats.
- Investigated suspicious activity, escalating incidents when necessary.
- Assisted in triaging and documenting security events and vulnerabilities.
- Supported senior analysts in incident response and digital forensics.
- Contributed to improving detection rules and dashboards.

Service Industry Roles - Server, Bartender, Cook — Various Employers

Austin, TX — *Fall 2020 - Present*

- Began working in the service industry at age 14, consistently maintaining employment while balancing academics, sports, social life, and volunteer work.
- Developed strong teamwork, leadership presence, and conflict-resolution skills in demanding, high-volume environments.
- Frequently trusted to train new staff and support management with guest issues, team communication, and shift structure.

Projects

Home Lab | *Network and Services* — Nov. 2025 - Present

- Ongoing project where I am designing and building a multi-device home lab to simulate an enterprise-style network for a full scale research environment for red, blue, and purple team operations on various systems/services.
- The home lab is isolated from my home network using a Netgate 1100 running a Pfsense+ firewall, Cisco Layer 3 managed switch, and a TP-Link edge router. Implementing VLANs, inter-VLAN routing, ACLs, firewall rules, etc.
- Developed a fully functional web application on a Raspberry Pi 5 by coding the front end (HTML, CSS, JavaScript) and back end (PHP, Node), integrating it with a MySQL database, and hosting it on an NGINX web server for a complete end-to-end deployment.
- Deployed and configured a BIND9 recursive and authoritative DNS server to manage custom internal hostnames. Optimized local traffic by implementing Access Control Lists (ACLs) and split-horizon DNS across multiple VLANs.
- Deployed an Active Directory Domain Services (AD DS) environment to simulate enterprise identity management. Configured Group Policy Objects (GPOs) for system hardening and implemented centralized logging (Sysmon/Windows Event Logs) forwarded to a SIEM to simulate threat hunting techniques.
- Actively expanding the lab to integrate additional enterprise services and security features.

Extracurriculars and Competitions

BASH | *University Cybersecurity Club* — Aug. 2025 – Present

- Secretary chair with responsibilities in handling internal communication and administrative tasks.
- Documentation, Tracking, and Event Support.

CCDC | *Collegiate Cyber Defense Competition* — Feb. 2026

- Defended and maintained a live enterprise-style network during an active Red Team attack, securing Windows/Linux servers, hardening services, and ensuring critical systems stay online.
- Identified, contained, and remediated real-time intrusions using log analysis, network monitoring, incident response procedures, and rapid system recovery techniques.
- Collaborated with a team to manage core infrastructure (AD, DNS, web, mail, databases), prioritize threats, and deliver clear executive-level reports under pressure.

Cyber 9/12 Strategy Challenge | *Atlantic Council* — Feb. 2026

- Selected to compete in the Cyber 9/12 Strategy Challenge, a national cybersecurity policy and strategy competition focused on responding to real-world cyber crises.
- Analyzed complex geopolitical and technical cyber scenarios, developed strategic response recommendations that balance national security, economic impact, and ethical considerations.
- Collaborated with a multidisciplinary team to brief judges on incident response strategy, risk assessment, and long-term cyber defense policy under time constraints.

CPTC | *Collegiate Penetration Testing Competition* Nov. 2025

- Conducted a network penetration test on simulated corporate network with production and development subnets.
- Collaborated with a team of 6 to conduct an 8-hour long penetration test, immediately followed by a 6-hour period to write the final report. Placed top 5.

TexSAW 2025 | *Cybersecurity conference and competition* Apr. 2025

- Hosted by the UT Dallas Computer Security Group (CSG).
- Participated in 48-hour CTF challenge among 410 teams from 26 countries.

Research Experience

Undergraduate Researcher Spring 2026 - Present

IoT Security and Vulnerability Research *Sam Houston State University*

- Full-Spectrum Vulnerability Research: Conducting comprehensive security audits of the various home ecosystems (IP cameras, home security systems, smart doorbells, etc.), analyzing attack vectors across RF (IoT-to-IoT), Network (IoT-to-Cloud), and physical hardware layers.
- RF Signal Analysis & Exploitation: Utilizing Software-Defined Radio (SDR) and YARD Stick One to intercept, demodulate, reverse engineer, and transmit proprietary Sub-1GHz radio protocols; investigating susceptibility to various attacks.
- Network Interception Infrastructure: Engineered a custom Man-in-the-Middle (MitM) research platform using a Raspberry Pi as an AP/Transparent Proxy capable of real-time traffic redirection, packet manipulation, connection downgrade, and malware injection.
- Protocol & API Analysis: Reverse-engineering communication between sensors, the Base Station, and Cloud APIs to identify flaws in authentication, data integrity, and command execution.

Technical Skills

Cybersecurity Red Teaming & Pentesting, Custom Malware Development, Vulnerability Research, Active Directory Attack/Defense. Familiar with a variety of tools/frameworks, such as BurpSuite, Metasploit Framework (Msfconsole/Msfvenom), Nmap, custom tools, etc.

Digital Forensics Hardware Forensics, Data Recovery & Acquisition, Memory Forensics, Artifact Analysis, Network Traffic Analysis (Wireshark).

Networking Enterprise Infrastructure (Firewalls, Managed L3 Switching, VLANs, Trunking), VPN Tunneling, Packet Crafting (Scapy), Deep Packet Inspection (DPI), MitM Frameworks, Rogue AP Setup.

Software Dev. Full-Stack Web/App Development (HTML, CSS, JavaScript, Php, C++, Java), Automation Scripting (Python, Bash, PowerShell), Version Control (Git), Database Management (SQL, NoSQL).