Chase Cooper

512-779-2142 | chasecooper393@gmail.com | github.com/CCoopSec | coopinfosec.com

Professional 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.

Research & Projects

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

- Designed and built 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. Actively expanding the lab environment.
- 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.

Smart Surveillance Systems Security Research Spring 2026 - Fall 2027

Empirical IoT Vulnerability Research *Independent*

- Full-Spectrum Vulnerability Research: Conducted comprehensive security audits of various home ecosystems (IP cameras, smart doorbells, etc.), analyzing attack vectors across RF (IoT-to-IoT), Network (IoT-to-Cloud), and physical hardware interfaces (e.g., UART, JTAG, SPI).
- RF Signal Analysis & Exploitation: Utilized Software-Defined Radios (SDRs) to intercept, reverse engineer, and transmit proprietary Sub-1GHz radio protocols, discovering susceptibility to Denial-of-Service (DoS) and targeted signal jamming.
- Network Interception Infrastructure: Engineered a custom Man-in-the-Middle (MitM) research platform using a Raspberry Pi as an AP/Transparent Proxy to perform real-time traffic redirection, packet manipulation, authentication downgrade, and malware injection.
- Hardware Debugging & Firmware Extraction: Interrogated undocumented debug interfaces (UART, JTAG, SWD) using logic analyzers and multi-protocol tools to gain privileged access, extracting embedded firmware via direct flash memory desoldering for offline static analysis.
- Vulnerability Disclosure & CVE Submissions: Authored PoC documentation for seven pending CVEs submitted to MITRE, detailing critical vulnerabilities across hardware debug interfaces, cryptographic usage, and network protocols.

Technical Skills

Languages: Python, C, C++, x86 Assembly, HTML/CSS/JavaScript, Bash Scripting, PHP, Node.js, SQL (MySQL/MariaDB), Java
Platforms & Infrastructure: Linux (multiple distributions), Windows Server, pfSense+, Active Directory (AD DS)
Security & Reverse Engineering: Wireshark, mitmproxy, Burp Suite, Caido, Splunk, Ghidra, GDB/Pwndbg, binwalk, QEMU
Hardware & RF Analysis: RTL-SDR, Yard Stick One, Bus Pirate, Logic Analyzers, Inspectrum, Universal Radio Hacker (URH), SDR#, XGecu Universal Flash Programmer
Certifications: CCNA (in-progress, Q1 2027), Security+ (in-progress, Q1 2027)

Competitions

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.

Capture The Flag (CTF) Competitions | *Various Platforms & Events* 2024 – Present

- Actively compete in numerous national and international CTFs, competing against hundreds of global teams.
- Develop and apply practical skills in reverse engineering, cryptography, network exploitation, and forensics under time-constrained scenarios.

Extracurriculars

Undergraduate Research Symposium Presenter | *Sam Houston State University* Apr. 2026

- Presented empirical research on the security posture and inherent vulnerabilities of IP-based video surveillance systems and consumer smart doorbells.
- Co-authored an empirical research paper alongside university faculty detailing hardware, network, and sub-GHz RF vulnerabilities targeted for IEEE publication.

BA$H | *University Cybersecurity Club* Aug. 2025 – May 2026

- Served as an executive officer organizing club initiatives and managing administrative operations.
- Delivered lectures and hands-on labs covering embedded device security, sub-GHz radio frequency analysis, and strategic approaches to CTF challenges.
- Helped 30+ students prepare for collegiate cyber defense and penetration testing competitions, and tutored them on network analysis, scripting, and programming fundamentals.

Education

Sam Houston State University Huntsville, TX
Bachelor of Science in Cyber Security *Aug. 2024 – May 2027*