

DAVIS BURRILL

C Y B E R S E C U R I T Y P R O F E S S I O N A L

CONTACT

-  +1 512 992 6658
-  davisburrill@icloud.com
-  Denver, CO 80203
-  [Davis Burrill LinkedIn](#)
-  [Davis Burrill Github](#)
-  <https://davisburrill.com/>

PROFILE

Curious and fast-adapting cybersecurity professional with a strong interest in both code and security. Completed a rigorous cybersecurity bootcamp at the University of Denver, gaining hands-on experience in Linux, Splunk, log analysis, and network security. Skilled in troubleshooting, scripting, and testing across various environments. Known for being a quick learner with a passion for building, breaking, and securing systems. Always eager to take on new challenges in a technical, team-driven setting.

SKILLS

PROGRAMMING

- Python, HTML, CSS, JavaScript

CYBERSECURITY

- Wireshark
- Kali Linux
- Metasploit
- Burp Suite
- Network Security
- Cryptography
- Security Operations

TECHNICAL PROJECTS

DEFENSIVE SECURITY LOG ANALYSIS (Splunk + SIEM Project)

Project | 2024

- Collaborated with a 6-person team to simulate a real-world defensive security environment for a fictional company, VSI, facing potential targeted cyberattacks.
- Set up and configured Splunk** to aggregate and analyze Windows Server and Apache web server logs.
- Developed **custom dashboards and alerts** to detect brute-force login attempts, account deletions, and HTTP POST floods from suspicious geolocations.
- Analyzed baseline vs. attack logs to identify high-severity anomalies, failed/successful login patterns, URI scans, and shifts in referrer domains.
- Created alert thresholds based on statistical baselines to minimize false positives and improve real-time detection of DDoS-style attacks.
- Delivered insights on log severity misclassification, evasion techniques, and attack attribution through structured reporting and visualizations.
- Proposed future mitigations including machine learning for anomaly detection, web application firewalls (WAFs), and continuous log refinement.

PURPLE TEAM AUTOMATION & THREAT DETECTION

Project | 2024

- Developed and deployed custom Python scripts to automate and enhance Nmap scanning, including spoofed scans and dynamic runtime configurations.
- Transformed raw XML scan outputs into timestamped, readable HTML reports for consistent QA documentation and log organization.
- Configured IDS/IPS tools including Snort and Security Onion for real-time alerting and threat detection using Zeek and Suricata.
- Created and tested Splunk alerts to flag suspicious login activity and monitor access logs for automated response.
- Reinforced defense with firewall rules (UFW) and mitigation strategies aligned with QA testing and monitoring objectives.

EDUCATION

CYBERSECURITY BOOTCAMP

University of Denver
June 2024 - December 2024

NEUROSCIENCE

University of Colorado Boulder
2016-2019

DAVIS BURRILL

CYBERSECURITY PROFESSIONAL

SKILLS

TECHNICAL

- Splunk
- Linux CLI
- Python & Bash
- Log Analysis
- WiFi Standards
- Docker
- Network Provisioning
- Alerting & Dashboards
- QA Testing ([pytest](#))
- Wireshark

CERTIFICATES

CompTIA Security+
CompTIA / 2024

CompTIA Network+ (in progress)
CompTIA

**Python Certified Associate
Programmer**
Python Institute / 2023

INTERESTS

- Cybersecurity CTF Challenges
- Software Development (especially Python and AI-driven apps)
- Snowboarding/Winter Sports
- Attending Colorado Sports

CYBERSECURITY BLOG & AZURE WEB APPLICATION

Project | 2025

- Designed and deployed a secure Python Flask web app using Docker containers on Microsoft Azure, hosted via GoDaddy.
- Implemented SSL certificates (self-signed & Azure-managed) and configured Azure WAF with geo-blocking rules to protect against unauthorized access.
- Used Linux-based tools and command-line utilities to manage deployment, troubleshoot issues, and monitor performance.
- Strengthened network and app security by remediating vulnerabilities using Azure Security Center and Microsoft Defender for Cloud.
- Created technical documentation and published CTF walkthroughs, demonstrating attention to detail, testing workflows, and root-cause analysis.
- Emphasized hands-on skills in **cloud deployment**, **web application hardening**, and **system-level QA testing**.

LANGCHAIN Q&A WEB APP

Project | 2025

- Built a full-stack document Q&A app using **LangChain**, **FastAPI**, and **React**, enabling users to upload files and ask context-aware questions.
- Wrote **automated tests using pytest** to validate backend logic, handle edge cases, and ensure endpoint reliability.
- Implemented thorough **error handling**, logging, and input validation to maintain a smooth user experience across the stack.
- Demonstrated end-to-end testing awareness, version control, and iterative debugging throughout development.

PROFESSIONAL EXPERIENCE

BARTENDER

Cherry Creek Grill | 2021-Present

- Maintained composure and attention to detail in a fast-paced, high-pressure environment.
- Demonstrated strong communication, multitasking, and problem-solving skills — now applying those to a cybersecurity and QA-focused career.
- Trusted with cash handling, time-sensitive decisions, and team collaboration during peak operations.