📍 Sykesville, MD

✉ c.jason11@outlook.com

✉Catherine.wunder89@icloud.com

🔗 linkedin.com/in/catherine-jason

💻 https://cjason0110.github.io/Catherine-Jason/

TECHNICAL STRENGTHS

• Networking

• Linux & Windows Administration

• Digital Forensics

• SIEM & Log Analysis

• Vulnerability Scanning

• Scripting

• Threat Analysis

TOOLS I USE

• Wireshark

• Nmap

• SNORT

• Splunk

• Nessus

• Metasploit

• Burp Suite

• Hashcat

CATHERINE JASON

SUMMARY

I'm Catherine Jason, a cybersecurity student pursuing an AAS in Cybersecurity with a 3.96 GPA and hands-on experience across networking, Linux administration, Windows Server, digital forensics, scripting, and security operations. I've configured Cisco Catalyst 2950, 2960 Plus, and 3560G switches, set up Cisco 4331 routers, administered Ubuntu Server, and managed Active Directory environments. I've also completed forensic investigations using E3 Forensic Platform, FTK Imager, OSForensics, and ProDiscover.

I've gained practical cybersecurity experience with tools like Wireshark, Nmap, SNORT, Splunk, Nessus, Metasploit, Hashcat, Aircrack-ng, Burp Suite, and Kali Linux, along with hands-on work in encryption, access control, and Bash scripting. My training includes the BCR Cyber Series and CompTIA-aligned A+, Network+, and Security+ labs, which strengthened my understanding of hardware, networking, and security fundamentals.

Outside of class, I enjoy building apps and websites in VS Code, experimenting with virtual machines, and learning through personal projects, cyber ranges, and platforms like TryHackMe. I'm preparing for roles in security operations, network defense, and digital forensics.

HANDS-ON EXPERIENCE

Network Infrastructure Build

• Configured Cisco Catalyst 2950, 2960 Plus, and 3560G switches

• Deployed Cisco 4331 ISR router with routing, NAT, and DHCP

• Implemented VLAN segmentation and inter-VLAN routing

• Performed packet analysis using Wireshark and SNORT

Linux & Windows Administration

• Aircrack-ng

• FTK Imager

• OSForensics

• ProDiscover

• E3 Forensic Platform

• Kali Linux

SYSTEMS & PLATFORMS

• Ubuntu Server & Desktop

• Windows Server / Active Directory

• Group Policy

• Virtual Machines

• GitHub Pages

• VS Code, IntelliJ, Eclipse

PROGRAMMING & SCRIPTING

• Bash scripting

• Java (OOP, debugging, pseudocode)

• HTML & CSS

CERTIFICATION-ALIGNED TRAINING

• CompTIA A+

• CompTIA Network+

• CompTIA Security+

• BCR Cyber Series

• TryHackMe & Cyber Ranges

• Managed Ubuntu Server and Desktop environments

• Configured Active Directory, Group Policy, and user permissions

• Performed system hardening and access control configuration

• Automated tasks using Bash scripting

Digital Forensics Investigation

• Conducted forensic imaging using FTK Imager and OSForensics

• Analyzed registry artifacts, email data, and file metadata

• Performed data carving and evidence recovery

• Documented findings following chain-of-custody standards

Cybersecurity Tools & Threat Analysis

• Executed vulnerability scans using Nessus

• Performed exploitation labs with Metasploit and Burp Suite

• Cracked password hashes using Hashcat

• Analyzed SIEM logs and alerts in Splunk

EDUCATION

AAS in Cybersecurity (In Progress)

Carroll Community College — Expected 2026

GPA: 3.96

Relevant coursework: Networking, Linux Administration, Windows Server, Digital Forensics, Intrusion Detection, Advanced Network Defense, Java Programming, Technical Documentation

PROFESSIONAL INTERESTS

I've never found a part of IT I didn't enjoy. Whether I'm configuring networks, analyzing logs, hardening systems, or digging into forensic data, I love the challenge and the learning that comes with every project.