TCHAIWANDA CHAMBERS

SYSTEM ADMINISTRATOR | CYBERSECURITY ENTHUSIAST

NEW HAVEN, CT | 2036194706 | TCHAIWANDA.CHAMBERS@GMAIL.COM

Professional Summary

System Administrator with 4+ years in IT and a growing specialization in cybersecurity. Experienced in managing Active Directory, firewalls, and endpoint protection. Currently building hands-on skills in threat detection, SIEM, and ethical hacking. Eager to contribute to a SOC team and grow within a security-focused role.

Experience

Cyrion | System Administrator **Present**

- Aided in security rules, configurations, and VPN policy implementation to enhance network security.
- Applied cybersecurity best practices to backup management, ensuring the availability and integrity of critical systems in line with NIST SP 800-34.
- Administered DNS records in Active Directory for network name resolution.
- Developed a PowerShell script to automate snapshot reports in VMWare environments.
- Managed vSphere virtual server farms, ensuring high availability and resource optimization.
- Provided support for virtual and physical infrastructure, troubleshooting performances.

Yale University | IT Support Technician 2 **September 2024 – February 2025**

- Managed and secured Active Directory, implementing user access controls, and security hardening best practices to mitigate insider threats.
- Managed device security using Microsoft Intune to enforce endpoint security policies.
- Resolved an average of 30+ support tickets per week, reducing system downtime by 25% through efficient troubleshooting and proactive maintenance.
- Provided technical support for Microsoft 365 security configurations (Teams, OneDrive, SharePoint).

Richemont NA | IT Helpdesk Analyst (Hybrid) **October 2023 – June 2024**

- Administered Azure AD security policies such as conditional access and identity management.
- Aided in securing POS solutions within SAP environments against unauthorized access.
- Enforced least privilege access by provisioning and deprovisioning user accounts.
- Helped with the deployment and maintenance of IT hardware and software applications.

Waterbury Hospital | Desktop Support Technician **August 2023 – October 2023**

- Installed, implemented and configured Sentinel One for endpoint protection.
- Resolved network and hardware issues to ensure consistent connectivity (Wi-Fi, DNS, IP conflicts).

Technical Skills & Core Competencies

- **Security & Compliance:** NIST SP 800-37, NIST SP 800-53, ITIL, IAM, Risk Management
- **Cybersecurity:** SIEM Tools, Threat Detection, Incident Response, Log Analysis, MFA, Linux Hardening, Vulnerability Scanning, Wireshark, Security Policies
- **Network Security:** Firewalls, VPNs, Conditional Access (WatchGuard)
- **Endpoint Security:** Sentinel One, ZScaler, Cisco VPN
- **Systems & Cloud:** Active Directory, vSphere, Microsoft Azure, VMware, Microsoft Intune, Windows Server, Windows AutoPilot
- **Scripting & Automation:** PowerShell, PowerCLI, Bash (Fundamentals)
- **Networking:** DNS, DHCP, TCP/IP, VLANs, VPNs, Routing & Switching
- **Operating Systems:** Windows, Linux, MacOS

Certifications

- **CompTIA Network+ (N10-009)** – *Issued: April 2025*
- **CompTIA Security+ (SY0-701)** – *Expected May 2025*
- **Google Cybersecurity Professional Certificate** – *Coursera / Google Career Certificates*
- **Introduction to Cybersecurity** – *Cisco Networking Academy*
- **Scrum Fundamentals Certified (SFC)** – *SCRUMstudy*

Projects

Wi-Fi Security Lab
ESP8266 Deauther & Isolated Network

- Created an isolated Wi-Fi lab environment using ESP8266 and Deauther firmware to safely explore wireless attack techniques and documented attack impacts on multiple test devices.
- Performed deauthentication, beacon spoofing, and MAC fingerprinting on test devices
- Practiced network segmentation and traffic isolation for ethical hacking purposes

Python-Based Port Scanner
Python, Nmap, Socket Programming

- Created a custom Python tool to scan network ports and identify open services on target hosts.
- Integrated Nmap for comprehensive scanning, service enumeration, and vulnerability insight.
- Demonstrated understanding of TCP/IP fundamentals and common reconnaissance techniques.

Virtual SOC Lab Simulation – Blue Team Practice
Kali Linux, Wireshark, Nmap, Netcat, Tcpdump

- Conducted packet analysis using Wireshark to detect anomalies and assess potential threats.
- Practiced hands-on exploitation and monitoring techniques using Kali Linux and open-source tools.

Network Infrastructure & Threat Analysis Lab
Virtual Networking, DHCP/DNS, Firewalls

- Configured virtual routers, switches, and firewalls to simulate enterprise-grade network environments.
- Implemented DHCP/DNS services and analyzed traffic flow to find potential vulnerabilities.

Linux Hardening Project on Mac Mini
Arch Linux, System Hardening, Linux Security

- Installed and secured Arch Linux on Mac Mini hardware, emphasizing lightweight performance and minimal attack surface.
- Applied essential Linux hardening practices including user privilege controls, firewall configuration, and secure boot setup.

Education

Post University | BSc Computer Information Systems

Relevant Coursework: Information Security, Network Security, System Administration, Cloud Computing, Virtualization

University of Connecticut | Full Stack Web Developer Bootcamp

Certification: UConn Coding Bootcamp - Certified Full-Stack Web Developer