GREY BREWER

Greater Denver Area
(303) 406-1055
greybrewer@outlook.com

https://www.linkedin.com/in/grey-brewer-bb8602204/

https://github.com/GBrew18/Grey_Brewer

OBJECTIVE

Outgoing and tenacious professional seeking my first hands-on Cybersecurity role with a team upon which I can grow and make an impact. I come highly recommended, am self-motivated, learn quickly, and bring positivity to every level of an organization. Whether operating as an independent contributor or collaborating within a team, I consistently strive to better myself, and happily help better those around me in the process.

RELEVANT EXPERIENCE

SEAKR Engineering - An RTX Company | Centennial, CO March 2025 – Present
IT Support Specialist (Full-Time, Onsite)

- Provide world class technical support to internal SEAKR/Raytheon employees, contractors, and guests via phone, email, chat, and in-person interactions.
- Perform step-by-step debugging and gather diagnostic details to ensure efficient and accurate issue resolution.
- Conduct basic network troubleshooting, including identifying connectivity issues, validating DNS, DHCP, and basic routing issues.
- Ensure Software/Firmware remains updated/patched, and all new installs are vetted and within compliance.
- Troubleshoot and resolve issues across mixed-OS environments, including Windows, Linux, and Solaris systems.
- Administer user accounts in Active Directory: creating new accounts, resetting passwords, and modifying group memberships.
- Assist with user onboarding/offboarding and access management in compliance with company policies and security best practices.
- Write and troubleshoot simple shell scripts (Bash and Batch) to automate routine system tasks.

- Respond to, assign, and manage support requests using a ticketing system (Request Tracker) while adhering to defined SLAs and escalation protocols.
- Collaborate with a cross-functional IT team to resolve multi-layered technical issues in a time-sensitive environment.
- Draft technical documentation and user-facing guides for internal knowledge bases to improve first-contact resolution.
- Prioritize and manage multiple support requests independently, while maintaining detailed records and follow-ups.
- Consistently recognized for professionalism and strong interpersonal skills when working under pressure and tight deadlines.

Stryker Site Services | Greenwood Village, CO May 2024 - March 2025
IT Support and Data Entry Technician - Part-Time
Stryker Site Services is a small, independent contractor for multiple large cellular carriers, among other clients.

- Successfully performed Windows 11 upgrade
- Performed full backup (2TB) of records via OneDrive, preventing future data loss
- Helped implement Yubikey 2FA for enhanced security to comply with T-Mobile's regulations
- Upgraded current PC's RAM, implemented Caldigit TS4 Docking Station, and installed dual-monitor setup to increase efficiency and reduce material costs (printing supplies, mainly)
- Assist with T-Mobile's VDI environment as needed
- Troubleshooting software, hardware, and peripheral issues on an on-call basis
- Support virtual conferencing platforms - Teams, Zoom, and Jitsi primarily
- Support the coordination of travel, as well as data entry using the MS 365 suite of tools.

CYBERSECURITY TRAINING / BOOTCAMP EXPERIENCE

University of Denver Cybersecurity Boot Camp

Completing a 24-week intensive, hands-on program emphasizing technical expertise in cybersecurity, systems administration, and network security to support and defend digital environments.

Key Achievements and Skills Gained:

- Security Fundamentals:
    - Applied the principles of the CIA triad to assess and secure information assets.

  - Designed governance, compliance, and disaster recovery plans to align with organizational goals.
  - Conducted detailed risk analyses, implemented risk mitigation strategies, and developed business continuity plans to minimize operational disruptions.
- Systems Administration:
  - Configured, hardened, and audited Linux and Windows servers to meet security best practices.
  - Automated administrative tasks using bash scripting, cron jobs, and logging tools to enhance efficiency.
  - Managed user authentication and access control with Active Directory and Kerberos, strengthening organizational security.
  - Gained proficiency in managing tar backups, process monitoring, and shell scripting for system optimization.
- Network Security:
  - Designed and implemented secure network architectures, focusing on protocols, data communication, and operational security.
  - Utilized tools like Wireshark to perform in-depth network traffic analysis and identify malicious activity.
  - Secured wireless communications and email systems, applying cryptographic methods for data integrity and confidentiality.
  - Conducted port scanning and explored virtualization and cloud security strategies to support scalable and secure infrastructure.
- Defensive Security (Current):
  - Leveraging SIEM tools like Splunk for continuous monitoring and advanced threat detection.
  - Developing incident response plans and executing simulated breach scenarios to mitigate threats.
  - Conducting forensic investigations, including data recovery and evidence preservation for legal proceedings.
- Offensive Security (Current):
  - Performing comprehensive penetration testing using industry tools such as Burp Suite, Zenmap, Searchsploit, and Metasploit.
  - Identifying and exploiting vulnerabilities, including SQL injection, XSS, file inclusion, and command injection, to highlight and mitigate potential risks.
  - Executing webshell deployments and network pivoting techniques to simulate advanced adversary tactics.
  - Strengthening web application security through vulnerability assessments and hardening protocols.
  - Preparing extensively for the CompTIA Security+ and Certified Ethical Hacker (CEH) certifications, ensuring a strong foundation in cybersecurity concepts and practices.

Summary of Experience:
This program has provided a comprehensive foundation in cybersecurity, emphasizing systems administration, threat detection, and mitigation across Linux and Windows platforms. The pursuit of mastery in both defensive and offensive techniques will hopefully ensure a well-rounded ability to secure, monitor, and test IT environments. With a strong focus on governance, network security, and hands-on implementation, this training has helped me bridge theoretical concepts and practical, hands-on application.

Homelab, Research, and Self-Study | November 2023 - Present
Intensive, hands-on study that combines physical hardware, software, and IT concepts that will translate to my next opportunity. Also includes preparation for CompTIA's Linux+, Network+, and Security+. Please see my GitHub for a full project portfolio.

Pi-Based Network/Security Monitoring Cluster:
Designed and deployed a multi-node Raspberry Pi cluster to serve as a network security monitoring and threat detection platform, utilizing industry-standard open-source security tools. This project integrates Intrusion Detection/Prevention (Suricata), Network Security Monitoring (Zeek), with future plans for a SIEM (Splunk) to analyze, log, respond to, and simulate network threats in real time.

Key Features & Technologies:

- Managed Network Segmentation & VLANs: Configured VLANs on a TP-Link managed switch to isolate security monitoring traffic, protect the home network, and ensure efficient IDS/IPS deployment.
- Intrusion Detection & Prevention (IDS/IPS): Deployed Suricata on a dedicated node to monitor and inspect live network traffic, generating alerts for suspicious activity and forwarding logs to a centralized SIEM.
- Network Security Monitoring (NSM): Integrated Zeek for deep traffic analysis, capturing metadata such as DNS queries, SSL certificates, and anomalous connections to provide forensic insight into network activity.

Future Nodes and Plans:

- Honeypot & Threat Intelligence: Can Deploy Cowrie and Dionaea honeypots to simulate vulnerable services, collect attacker fingerprints, and feed intelligence into security analytics platforms.
- Centralized Security Information & Event Management (SIEM): Will configure Splunk to aggregate security logs, analyze attack patterns, and visualize network activity with real-time dashboards.

- Automated Log Collection & Retention: Implemented Docker containers across the cluster for automated log forwarding and data retention, ensuring persistence across system reboots and network changes.
- Cloud & Virtualization Concepts: Designed the cluster with containerized services using Docker and Docker Swarm/Kubernetes, mimicking cloud-based security architectures.

This project has provided me real-world, enterprise-relevant experience in cybersecurity monitoring, intrusion detection, and network forensics, simulating a Security Operations Center (SOC) environment on a scalable, modular, and cost-effective Raspberry Pi cluster. The cluster will serve as platform to continue learning the following technical skills:

- Network Security & Traffic Analysis (IDS/IPS, NSM, Packet Capture, Threat Hunting)
- Linux System Administration (Ubuntu Server, Rocky Linux, Fedora, Bash Scripting, Log Management)
- Embedded Linux and IoT Research (Kernel Development, Yocto Project, Firmware Analysis,
- Infrastructure Automation (Docker, Vagrant, Ansible for Configuration Management)
- Networking & Virtualization (VLANs, Managed Switch Configuration, Packet Mirroring, Port Forwarding)
- Security Operations & SIEM (Splunk, Honeypots, Digital Forensics/Incident Response)

Sample of Hands-On Labs Completed - TryHackMe

Web Hacking, Offensive Security Tooling, Exploitation Basics

Completed over a dozen hands-on labs simulating real-world penetration testing scenarios across web exploitation, offensive tooling, and post-exploitation tactics.

- **Web Application Basics** – Learned HTTP methods, request/response structure, status codes, and headers critical to web reconnaissance and manual testing.
- **JavaScript Essentials** – Explored how client-side scripts introduce attack vectors such as DOM-based XSS and how attackers manipulate browser behavior.
- **SQL Fundamentals** – Practiced writing SQL queries and understood how poor input validation leads to SQL Injection vulnerabilities.
- **Burp Suite: The Basics** – Used Burp Suite to intercept and manipulate HTTP traffic, test for input handling flaws, and identify insecure session management.
- **OWASP Top 10 – 2021** – Studied critical web application risks, including Injection, Broken Authentication, Sensitive Data Exposure, and Security Misconfiguration.
- **Hydra** – Performed credential brute-force attacks on services like SSH and HTTP using tailored wordlists.

- **Gobuster: The Basics** – Conducted enumeration of hidden web directories and files using wordlist-based discovery for reconnaissance.
- **Shells Overview** – Differentiated between bind, reverse, and web shells; learned their use in gaining remote access and persistence on compromised systems.
- **SQLMap: The Basics** – Automated SQL Injection attacks using SQLMap, including database fingerprinting, data extraction, and login bypasses.
- **Moniker Link (CVE-2024-21413)** – Exploited a real-world Outlook vulnerability to leak credentials by bypassing Protected View via malicious link execution.
- **Metasploit: Introduction & Exploitation** – Gained practical experience using Metasploit for vulnerability assessment, module selection, and system exploitation.
- **Metasploit: Meterpreter** – Used Meterpreter to execute in-memory payloads, upload/download files, escalate privileges, and maintain access stealthily.
- **Blue** – Performed full compromise of a vulnerable Windows 7 machine by exploiting SMB vulnerabilities and misconfigurations using Metasploit.

Please see my GitHub for the latest in my project portfolio.

TP-Link Router Exploitation: A Beginner's Attempt at Hardware Hacking
https://medium.com/@greybrew18/tp-link-router-exploitation-a-beginners-attempt-at-hardware-hacking-274c0125282c

OTHER RELEVANT EXPERIENCE

Compri Consulting | Denver, CO Mar 2023 – Sep 2024
Technical Recruiter - Remote
Position eliminated given downward job market

- Performing the end-to-end recruitment process, including posting job openings, sourcing candidates, reviewing resumes, conducting initial phone screens, and coordinating interviews.
- Conducting initial candidate assessments to evaluate qualifications, skills, and cultural fit.
- Support the coordination of interview schedules and act as liaison for communication with candidates.
- Ensure a positive candidate experience by providing timely communication, feedback, and information about the company culture and values
- Utilize tools like Dice, LinkedIn Recruiter, Bullhorn ATS, Adobe Acrobat, LibreOffice, and MS Office.

Compri Consulting | Denver, CO July 2022 – Mar 2023
Technical Sourcer
Compri Consulting is an IT staffing company that has been around since 1992. We work with clients spanning all kinds of industries such as healthcare, utilities, finance, robotics, manufacturing, insurance, software, government and more. We staff the whole gambit of IT-from helpdesk all the way up to executives, in areas ranging from software development, project/product management, business analysis, QA, and more. We work with startups as well as Fortune 500 companies. We are based in Denver but work with clients all over the country, with a concentration of business here in Colorado.

- Acted as initial point of contact for highly qualified candidates before introducing them to the recruiter for respective job opportunities.
- Successfully sourced over 10 placements within the first 6 months.
- Utilized Dice, LI Recruiter, Bullhorn ATS, and MS Office to source / track candidates.

Valley Country Club | Aurora, CO Feb 2016 – July 2022
Golf Operations Supervisor & Lead Junior Golf Instructor

- Providing optimal member experience, I built meaningful and lasting relationships with members through a genuine service-oriented attitude, strong interpersonal skills, and vast knowledge of the game of golf.
- Served as lead Junior Golf Coach for multiple years. Organized, planned, and taught Junior Golf curriculum, ensuring other instructors felt empowered and prepared to teach.
- Effectively used MS Office Suite to make schedules, presentations, spreadsheets, posters, scoreboards, as needed.
- Successfully used and troubleshot POS system to ensure smooth transactions and accurate record keeping.

EDUCATION

Cybersecurity Bootcamp | Online Sept 2024-Mar 2025
University of Denver (Please see below for curriculum)
CompTIA Security+ | Self-Study Jun 2025
https://www.credly.com/badges/e5ad6c7e-0524-41a8-b017-aa0bb2fb8228/public_url
CompTIA Linux+ | Self-Study Jun 2024
https://www.credly.com/badges/90706fa1-a3ac-4870-b14c-f48117aa1a8b/public_url
CompTIA Network+ | Self-Study March 2025
https://www.credly.com/badges/b52e55a1-7173-446f-8d87-a74bf2510228
CompTIA CLNP | Self-Study March 2025
https://www.credly.com/badges/17d9ee70-81b7-412a-9047-f9d784d9693c

Tabor College | Hillsboro, KS 2020-2021
Coursework in Psychology and English
Embry-Riddle University | Prescott, AZ 2018-2019
Coursework in Aerospace Engineering

SKILLS

- Troubleshooting (Networking, OS, Hardware, Storage)
- Command-Line Interface
- Professional and kind communication skills
- Basic Windows and Linux Administration (Multiple Distros / Package Managers)
- Active Directory
- System hardening/auditing, reconfiguration, and log review
- Windows 10 and 11
- CentOS, RHEL, OpenSUSE, and Ubuntu
- Wireshark and Zeek for network monitoring
- Proficient in Metasploit, Burp Suite, and John the Ripper
- C2 Frameworks, OWASP Top 10, and MITRE ATT&CK
- Basic understanding of UART / JTAG / SPI interfaces
- Python 3 - basic proficiency but continue to learn through projects
- MS Office, Request Tracker (RT),
- Remote Server and Desktop Support (SSH, RDP, VDI tools, etc)
- Relationship building and customer service
- Highly organized with strong attention to detail
- Passion for efficiency and learning
- Deep sense of integrity and desire for exceeding competency

INTERESTS

- **Golf:** Played collegiately and Skilled Instructor/Coach
- **Technology:** Linux, Hardware Hacking, Raspberry Pi, Networking, DevOps, Cyber Security, 3D Printing, General Computer Science
- **Outdoors:** Fishing, hiking, exploring new trails with my dog
- **Community:** Given Community Service Award in 2015 from City of Centennial