Matthew Nebiyou

matthew.nebiyou@gmail.com · (301) 357-9958 · mnebiyou.com

CompTIA Security+ Certified (2026)

PROFESSIONAL SUMMARY

CompTIA Security+ certified professional transitioning into cybersecurity from a background in data analysis and biomedical research. Led an authorized penetration test on a live business network, gaining full administrative access to 30 networked security cameras and other exposed devices, then designed and deployed the segmented network that remediated every finding. Deployed a Wazuh SIEM providing continuous vulnerability and log monitoring across production systems, catching real-world CVEs missed by manual review. Brings six years of data analysis and cross-bureau stakeholder reporting experience, translating technical findings into clear guidance for non-technical audiences.

TECHNICAL SKILLS

Offensive Security: Penetration testing, Nmap, Nikto, Burp Suite, SQLmap, Metasploit, OWASP Top 10

Defensive / SIEM: Wazuh, IDS, log analysis, vulnerability management, vulnerability assessment, CVE triage, Fail2ban

Networking: OPNsense, VLANs, firewall rules, Tailscale / WireGuard, network segmentation, managed switching

Systems: Linux, Bash, Python, SELinux, Docker Compose, Terraform, LUKS encryption, RAID, firewalld, SSH hardening

Data & Analysis: Data analysis, Excel, technical writing, stakeholder reporting

HOMELAB PROJECTS & SECURITY RESEARCH

Authorized Network Pentest & Full Remediation | Small Business — Coffee Shop *Personal Project*

- Conducted a scoped 2-hour penetration test on a live flat network, gaining full admin access to 30 networked IP cameras via shared default credentials, exposing POS systems and staff devices to any device on the guest Wifi
- Identified 3 Clover POS terminals and other IoT devices sharing that same unsegmented network; delivered a severity-rated findings report in plain language for the non-technical owner and reset credentials on all 30+ affected devices
- Eliminated the attack surface by designing and deploying a replacement network, OPNsense firewall on a repurposed Dell OptiPlex, managed switch, and three isolated VLANs (guest/staff/IoT-camera) with default-deny inter-VLAN rules

Wazuh SIEM — Security Monitoring & Vulnerability Detection | Self-hosted Homelab *Ongoing*

- Deployed the full Wazuh stack (manager, indexer, dashboard) via Docker Compose for continuous vulnerability scanning and log monitoring across a production Linux server and the network's edge firewall
- Vulnerability scanning surfaced real-world CVEs missed by manual review, including high-severity findings in pyasn1 and pycrypto; verified each against the NVD and removed the affected packages, closing the exposure
- Used the OpenSearch-backed Wazuh Dashboard for alert triage and severity-based vulnerability prioritization, surfacing supply-chain dependency risk invisible to manual review

Self-Built Home Server & Penetration Testing Lab | Self-hosted Homelab *Ongoing*

- Built and maintain a headless Fedora Server hardened with LUKS full-disk encryption, RAID 1 redundancy, enforcing-mode SELinux, and Tailscale-only SSH access
- Deployed Tailscale with MagicDNS and Funnel for secure public HTTPS exposure of select services, keeping zero open ports on the router
- Configured and operate a 4-container isolated pentest lab (DVWA, OWASP Juice Shop, WebGoat, bWAPP) to practice SQL injection, XSS, command injection, file inclusion, and broken authentication using Nmap, Nikto, SQLmap, and Burp Suite

WORK EXPERIENCE

Data Analyst | DC Health *Jul 2023 – Present*

- Led integration of new data technologies across three divisions within the Bureau, streamlining mission-critical workflows and improving reporting consistency for senior leadership
- Reviewed and synthesized a ~10-program population health portfolio into recurring data updates for senior Bureau leadership
- Collaborated across bureaus in cross-functional forums (CoP, DAWG, C_DAWG) to establish and improve data governance practices spanning collection, management, maintenance, and analysis
- Delivered monthly Data & IT updates to Bureau leadership and provided technical assistance to program staff

Postbaccalaureate Fellow | National Institutes of Health *Aug 2020 – Jul 2023*

- Designed and ran novel in vitro experiments using induced pluripotent stem cells (iPSCs) to investigate molecular mechanisms underlying neurodegeneration in ALS, Alzheimer's, and Parkinson's disease
- Analyzed structured experimental data using Excel and GraphPad Prism, contributing to findings published in three peer-reviewed journals, including Nature Communications and Neuron
- Automated unstructured image-analysis pipelines using FIJI for routine and specialized workflows, reducing manual processing time and accelerating delivery of neurodegeneration research findings
- Used RStudio to transform and visualize experimental data, surfacing insights that corroborated and extended existing findings

EDUCATION

BS — Biochemistry, Molecular Biology & Bioinformatics | Towson University *Dec 2019*

summa cum laude — computational analysis, biological data pipelines

Full project documentation, architecture diagrams, and write-ups: mnebiyou.com/projects