Matthew Nebiyou

matthew.nebiyou@gmail.com · (301) 357-9958 · mnebiyou.com *CompTIA Security+ (in progress)*

Analytically driven professional transitioning into cybersecurity with hands-on homelab experience across offensive security, defensive monitoring, network engineering and Linux systems administration. Conducted an **authorized penetration test on a live business network**, identified critical vulnerabilities and personally built the remediated network infrastructure. Deployed a **Wazuh SIEM** that detected and led to the removal of real CVEs from a live system. Background in data analysis and scientific research brings rigorous investigative thinking and clear communication of technical findings to 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, CVE triage, Fail2ban
Networking: OPNsense, VLANs, firewall rules, Tailscale / WireGuard, network segmentation, managed switching
Systems: Linux (Fedora Server), SELinux, Docker Compose, 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 pentest on a live flat network; gained **full admin access to all Lorex IP security cameras via default credentials** from the guest WiFi, demonstrating critical exposure of POS systems, staff devices and cameras to any customer on the network
- Produced a **structured findings report** with severity ratings and plain-language risk descriptions for non-technical business owners; changed default credentials on all affected devices during the engagement
- Designed and built a replacement network: **OPNsense firewall** on a repurposed Dell Optiplex, managed switch, three isolated VLANs (guest / staff / IoT-cameras), separate SSIDs per segment and finally explicit inter-VLAN deny rules enforcing default-deny policy

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

- Deployed the **full Wazuh stack** (manager, indexer and dashboard) via Docker Compose; installed a host agent on Fedora Server for real-time system monitoring and CVE scanning against the National Vulnerability Database
- Vulnerability scanner detected **real CVEs in installed packages** including a high-severity finding in pyasn1 and severe finding in pycrypto: transitive dependencies not deliberately installed; verified against NVD and removed affected packages from the live system
- Used the OpenSearch-backed Wazuh Dashboard for **alert triage**, vulnerability prioritisation, and log analysis — demonstrating the value of automated scanning for supply chain dependency risks invisible to manual review

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

- Built and maintain a headless Fedora Server on a self-assembled AMD FX-8320 desktop; implemented **LUKS full-disk encryption** on the boot drive, software RAID 1 for data redundancy, SELinux in enforcing mode and SSH restricted to Tailscale-only access
- Deployed a **Tailscale zero-trust mesh network** with MagicDNS and Tailscale Funnel for secure public HTTPS exposure of select services — zero open ports on the router at all times
- Built and operate a four-container pentest lab (DVWA, OWASP Juice Shop, WebGoat, bWAPP) on an isolated Docker bridge network; practiced **SQL injection, XSS, command injection, file inclusion** and broken authentication using Nmap, Nikto, SQLmap, and Burp Suite

WORK EXPERIENCE

Data Analyst | *DC Health* 2023 – Present

- Managed the integration of new technologies across Divisions to complement and enhance mission-critical workflows
- Led periodic reviews of the Bureau's population health portfolio and collated important data-related updates to be included in timely reports for senior CHA leadership.

- Collaborated with stakeholders across bureaus in multiple forums (CoP, DAWG, C_DAWG) to establish new (and improve existing) rules of practice and procedure as it pertains to data collection, management, maintenance, and analysis across CHA.
- Conducted *Data and IT Updates* portion of monthly Bureau meetings as well as provided TA to program staff to build capacity

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

- Conducted novel *in vitro* experiments using induced pluripotent stem cells (iPSCs) to investigate the molecular mechanisms underlying neurodegeneration as it pertains to ALS, Alzheimer's Disease and Parkinson's Disease.
- Automated unstructured data analysis pipelines using FIJI for both routine and specialized analysis, saving both time and energy from lengthy and tedious analysis.
- Analyzed structured *in vitro* experimental data using Microsoft Excel and GraphPad Prism for inclusion in multiple publications on neurodegeneration development.
- Utilized RStudio to transform and visualize data, gleaning new insights that were either previously unknown or corroborated established information, thus leading to further knowledge gain.

EDUCATION

BS — Biochemistry, Molecular Biology & Bioinformatics 2019

Towson University · summa cum laude — computational analysis, biological data pipelines

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