Micah Nelson

mngrateful@gmail.com • 862-867-0321 • linkedin.com/in/micah-a-nelson/ • github.com/micah-0w0

SUMMARY

SANS-trained cybersecurity practitioner with experience in system security, log and packet analysis, and multi-tool investigation across Windows and Linux environments. Brings strong analytical skills, structured documentation, and a methodical approach to investigating alerts with clarity and precision.

SKILLS

Security Analysis: Incident response, log analysis, packet analysis, Windows/Linux hardening, access control & authentication, malware triage, memory forensics, vulnerability analysis, web security, cloud security
Tools: Wireshark, Nmap, SIEM (Splunk, ELK), Windows Event Viewer, Sysinternals, Autopsy, FTK Imager
Networking & OS: TCP/IP, DNS, HTTP/HTTPS, Linux (Ubuntu, Debian, Kali, CentOS), Windows 10/11/XP
Programming: Python, Java, C, PowerShell, Bash

EDUCATION & CERTIFICATIONS

Northeastern University, Oakland Campus **Expected May 2030**
Bachelor of Science in Computer Science

SANS Cyber Academy **January 2026 – July 2026**
Certifications: GIAC Certified Incident Handler (GCIH), GIAC Security Essentials Certification (GSEC), GIAC Foundational Cybersecurity Technologies Certification (GFACT)

CYBER PROJECTS & ENGAGEMENT

SANS Cyber Academy **January 2026 – July 2026**

- Completed 60+ security labs, investigating Windows, Linux, and network-based attacks using Wireshark, Tcpdump, Sysinternals, Windows Event Viewer, and command-line tools.
- Performed incident response investigations across simulated enterprise environments, analyzing host artifacts, logs, and network traffic to identify indicators of compromise and attacker activity.
- Investigated attacker techniques including exploitation, privilege escalation, persistence, and lateral movement, developing practical incident-handling skills validated by GSEC and GCIH certifications.

US Cyber Challenge Cyber Camp **June 2026**

- Completed 45 hours of intensive cybersecurity training across four technical courses covering cybersecurity program analysis, mobile device forensics, malware analysis, and Linux forensics.
- Conducted mobile forensics investigations using FTK Imager, Autopsy, ADB, iBackUpBot, and SQLite DB Browser to recover deleted artifacts, analyze backups, and reconstruct user activity timelines.
- Performed Linux forensics analysis using Volatility and command-line tools to identify malicious processes, review credential artifacts, and detect an LD_PRELOAD rootkit on a compromised system.

TryHackMe Cybersecurity Labs **November 2024 – Present**

- Completed 170+ hands-on labs across Linux, Windows, networking, web/cloud security, and incident response fundamentals, strengthening practical troubleshooting and investigation skills.
- Utilized Splunk and ELK to query, filter, and correlate security logs during hands-on labs, investigating brute-force attempts, anomalous DNS activity, unauthorized access, and common SOC alert scenarios.

New Jersey Governor's School of Engineering and Technology Research **July 2024**

- Developed a Python-based Binary Ninja plugin to automate simplification of obfuscated C programs, reducing manual reverse-engineering time and improving analysis consistency.
- Presented IEEE Xplore publication at the MIT Undergraduate Research Technology Conference.

RELEVANT EXPERIENCE

Somerset Hills YMCA **July 2026 – August 2026**
Administrative Intern Basking Ridge, NJ

- Managed daily operations by preparing 100+ packets, organizing equipment inventories, and maintaining Excel spreadsheets to ensure accurate records and inventory tracking.
- Recorded attendance for 100+ classes, supporting budget analysis and reporting.
- Supported member communication by registering 40+ personal training programs, coordinating scheduling with members, and editing outreach emails to improve clarity and engagement.

FIRST Robotics Team 9116 **September 2021 – June 2025**
Captain & Lead Programmer North Plainfield, NJ

- Troubleshot software, hardware, and connectivity issues, coordinating rapid fixes in competitions.
- Standardized GitHub repositories and documented workflows for repeatable issue resolution.
- Coordinated software integration with mechanical/electrical systems for reliable robot performance.