Yao Prosper Amebe

240-351-4031 • Silver Spring, MD • prosperamebe14@gmail.com • GitHub • LinkedIn • Portfolio

PROFESSIONAL SUMMARY

Cybersecurity professional with 2+ years of software development experience and a strong foundation in offensive security techniques. Demonstrated hands-on red team skills through competitive CTFs. 2nd place at the Maryland HTB CTF, 21 objectives at SANS Holiday Hack challenge, and top 6% ranking in the NCL. Experience in web application exploitation, network reconnaissance, and reverse engineering. CompTIA Security+ and Linux+ certified.

CERTIFICATIONS

CompTIA Security+ — Issued Sep 2025 • **CompTIA Linux+** — Issued Jun 2025

TECHNOLOGY & SKILLS

Security Operations & Pentesting: Burp Suite, Nmap, Netcat, HashCat, John the Ripper, Wireshark, Kali Linux, OpenVAS, Metasploit, Tshark.
Digital Forensic & Intel: Autopsy, FTK imager, Volatility, Binwalk.
Networking & Protocols: DNS, DHCP, TCP/IP, VLANs, Firewall, Subnetting, Packet Analysis.
Platforms & OS: Ubuntu, Windows Server, Active Directory, Azure, AWS, Google Cloud Platform, VirtualBox,
Programming & Scripting: Python , Bash, PowerShell, Dart, C++, Java, JavaScript.
Frameworks & Standards: MITRE ATT&CK, NIST CSF, OWASP Top 10, Git/GitHub.

PROJECTS & CTF

National Cyber League *Jan. 2026 — April 2026*

- Ranked 214th out of 3,634 teams nationwide while competing across Web Application Security, Enumeration &Exploitation, Log Analysis, Network Traffic Analysis, Forensics, OSINT, Cryptography.
- Achieved 100% completion in Scanning & reconnaissance challenges using Nmap, Netcat, identifying vulnerable services on a target host and enumerating an IoT network via MQTT to extract IOC.
- Identified web application vulnerabilities and automated log analysis tasks with python scripts.

Spring 2026 Maryland HTB CTF

- Led Montgomery College's team to 2nd place overall, earning 9.325 points and 19 of 27 flags across Digital Forensics, Web Exploitation, Reverse Engineering, OSINT, and Secure Coding.
- Identified a Server-Side Request Forgery (SSRF) vulnerability through source code analysis and implemented a fix.

SANS Holiday Hack Challenge 2025 | Write-ups: https://prosmaw.github.io/sans-holiday-hack-challenge2025/

- Completed 21 objectives across network analysis, cloud security, web exploitation, and reverse engineering.
- Exploited IDOR vulnerabilities, performed RCE with privilege escalation, and bypassed authentications
- Exploited JWT/JWKS authentication weakness by generating RSA key pairs with OpenSSL and forging trusted tokens to bypass authorization controls.

RELATED EXPERIENCES

Student Assistant | Montgomery College | Germantown, MD *Dec. 2024 — May 2026*

- Taught networking protocols, Active Directory configuration, and VM setup to 2 to 4 students per shift with exposition to enterprise infrastructure commonly targeted in red team activities.
- Tutored Python and C++ programming with 90% + of recurring students showing grade improvement, reinforcing low-level programming and logic skills applicable to exploit development and tooling.

Software Developer | Social Informatic | Lome, Togo *Jan. 2023 — Dec. 2023*

- Integrated RESTful APIs with token-based authentication over HTTPS, participated in architecture decisions around data minimization and JWT token handling, gaining practical understanding of API design.

EDUCATION

Associate of applied science in Cybersecurity | GPA: 3.90
Montgomery College — Germantown, MD *Jan. 2024 — May 2026*

Bachelor of Science in Computer Science
University of Lomé — Lomé, Togo *Nov. 2019 — Dec. 2023*