MUSE ABDULRAHMON OLANIYI

Cybersecurity & IT Support Analyst

10cloudstechnology@gmail.com | +2348075437692
Lagos, Nigeria

LinkedIn: linkedin.com/in/muse-abdulrahmon/
GitHub: github.com/Nightowl36373838/Python_owl
Medium: medium.com/@Muse_abdulrahmon

PROFESSIONAL SUMMARY

As a cybersecurity enthusiast and IT professional, I am eager to contribute my technical skills to a forward-thinking organization while supporting secure and efficient technology operations. I specialize in bridging the gap between efficient **IT operations and robust security protocols**. With a solid foundation **in Linux and windows environments** and a passion for VAPT (Vulnerability Assessment and Penetration Testing), I look for ways to make systems more resilient and I am excited to bring this security-first approach, supporting both the **internal infrastructure and the innovators** who rely on it.

EDUCATION & CERTIFICATIONS

B.Sc. in Microbiology – Lagos State University — August 2020 – October 2024

Diploma in Ethical Hacking – Alison — November 2022

CCNA CyberOps Associate — March 2025

Aviatrix Certified Engineer – MultiCloud Network Associate — September 2025

Certified Associate Penetration Tester (CAPT) – Hackviser — October 2025

EXPERIENCE

OMD Tech Communication – Lagos, Nigeria
Student Engineer — March 2019 – October 2021

- Installed and maintained Windows 7–11 systems across multiple user environments, ensuring reliable performance and minimal operational disruption.
- Recovered data from corrupted hard drives, USBs, and memory cards using forensic tools.
- Restored access to locked or inaccessible Windows systems using authorized recovery techniques, reducing user downtime and secure restoration of user access.
- Utilized reverse engineering tools (x64dbg) to analyze application binaries, identify root causes of failures, and improve system reliability.
- Diagnosed and resolved system performance issues by applying registry fixes, updating drivers, and fine-tuning hardware configurations.

SAP Cybersecurity Engineering Virtual Internship Program – Forage
Cybersecurity Analyst Intern — January 2023

- Detected and mitigated phishing attempts via email, SMS, and document vectors.
- Conducted password policy compliance checks to reduce credential-based risks.
- Delivered a professional report highlighting security gaps, strengths, and recommendations for organizational security improvement.

RedOps Starter Camp – Remote

Founder/Instructor-Lead — June 2025 – July 2025

- Founded and directed the RedOps STARTER CAMP, a 1-month cybersecurity bootcamp that provided hands-on training to over 100 students.

- Trained participants through a hands-on curriculum, delivering recorded sessions on over 60 Kali Linux commands and leading live labs on phishing, network reconnaissance, and social engineering.
- Successfully implemented a system to manage student progress and automate the distribution of secure, verifiable certificates and transcripts.
- Reinforced theoretical knowledge with practical application, guiding students through a series of weekly assessments on the TryHackMe platform to solidify their red and blue team skills.

Warri Tech Hub – Warri, Delta State

IT & Cybersecurity Facilitator / IT Operations Support January 2026 – November 2026 (Ongoing)

- Delivered structured IT and cybersecurity training while designing hands-on labs in networking and security, equipping 20+ learners with practical, job-ready skills and improving engagement and knowledge retention.
- Managed end-to-end IT support operations, troubleshooting hardware, software, and network issues while optimizing systems, contributing to improved operational efficiency, reduced downtime, and enhanced user satisfaction.
- Installed, configured, and maintained network infrastructure, including router setup, structured LAN cabling, and internal/external deployments, ensuring reliable connectivity across organizational and client environments.
- Deployed and supported wireless bridge networks using NanoStation (point-to-point) technology, delivering connectivity to 10+ client locations, expanding service coverage and enhancing network accessibility.

SKILLS

Tools & Frameworks: Nmap, Burp Suite, Metasploit, AnyDesk, Nessus, Wireshark, TeamViewer.
Domains: Penetration Testing, Vulnerability Scanning, IT Operations, Infrastructure Security, Network Security.
Operating Systems: Linux (Kali, Ubuntu, Tails), Windows (7–11), Windows Server, VMware workstation.
Programming & Scripting: Python, Powershell.
Soft Skills: Communication, Problem-Solving, Team Collaboration, Critical Thinking.

PROJECTS

Phishing and Social Engineering Campaign Simulation

Engineered a simulated phishing campaign using the SEToolkit framework to test security awareness and tracked user interactions and provided a detailed report outlining the campaign's success rate and offering recommendations for improving organizational security awareness.

Network Vulnerability Assessment & Mapping

I conducted a comprehensive scan of a controlled lab environment to identify open ports and outdated services using Nmap and Nessus. I generated a detailed risk report prioritizing vulnerabilities based on CVSS scores and provided remediation steps to harden the network perimeter.

Web Application Security Testing

Used Burpsuite, SQLmap, OWASP ZAP to perform manual and automated security testing on a mock e-commerce application to identify flaws such as SQL Injection (SQLi) and Cross-Site Scripting (XSS), then i successfully intercepted and modified HTTP traffic to bypass authentication, demonstrating the business impact of insecure code and recommending secure coding practices.