Obah Emmanuel

6, Michael Igbudu Street
Greenfield Estate, Amuwo-Odofin
Lagos State, Nigeria
(+234) 912-468-1474
eobah105@gmail.com
[Linkedin](#) | [Github](#)

Professional Summary

I'm an aspiring Security Analyst with hands-on experience in cybersecurity tools like Nmap, Wireshark, Wazuh, and Kali Linux. I have a strong understanding of security fundamentals, including least privilege, vulnerability assessment, risk management, and IAM. I've completed virtual internships in Identity and Access Management (TATA) and Vulnerability Management (AIG) and am eager to gain real-world experience through an internship to further develop my skills.

Certifications

- **ISO/IEC 27001 Certified**
- **ISC2 Certified in Cybersecurity (Exam Passed, Certification Pending)**
- **Cisco Introduction to Cybersecurity**
- **CompTIA Security+ (Studied, Expected Certification: September 2025)**

Technical Skills

- **Security Operations: SIEM tools, IDS/IPS, Incident Response, Threat Detection**
- **Networking & Security: Nmap, Wireshark, Suricata, Firewall Configuration**
- **Identity & Access Management (IAM): SSO, Access Control, Authorization Models**
- **Programming & Automation: Python (basic), Bash (basic), Security Scripting**
- **System Administration: Linux (Ubuntu, Kali), Windows Security Monitoring**

Projects

Major Projects

[Malware Analysis](#)

- **Conducted static and dynamic analysis of malware samples.**
- **Reverse-engineered malicious binaries to identify indicators of compromise (IOCs).**
- **Utilized tools like PE Studio, Wireshark, and Procmon for in-depth threat assessment.**

[Wazuh Security Lab](#)

- **Built a security monitoring lab using Wazuh for SIEM and threat hunting.**
- **Implemented FIM to monitor sensitive directories.**
- **Simulated an SSH brute-force attack and a Kali Linux container to analyze security events.**
- **Integrated TheHive for Security Orchestration, Automation, and Response.**

Mini Projects

[DOS Attack Response](#)

- Used Nmap for network reconnaissance to find target hosts on the network.
- Launched an ICMP flood attack to simulate a DoS attack.
- Used Wireshark to detect and analyze Denial-of-Service (DoS) attempts.
- Configured firewall rules to mitigate malicious traffic.

Phishing Email Simulator

- Designed and implemented a phishing simulation tool to raise awareness.
- Created realistic phishing emails mimicking common cyber threats.
- Analyzed responses and educated users on identifying phishing attempts.

Experience

Forage Cybersecurity Simulations

TATA Consultancy Services – IAM Fundamentals

- Designed and implemented an Identity and Access Management (IAM) plan.
- Gained hands-on knowledge of SSO, access control models, and authorization mechanisms.

AIG Cybersecurity Virtual Internship

- Used CISA's documentation to research vulnerabilities and practiced vulnerability management.
- Created a Python script to brute-force a file encrypted by ransomware.

Education & Training

Bachelor's Degree in Computer Science (First-Year Student)
University of Ibadan

- Self-taught with a strong passion for cybersecurity and ethical hacking.
- Ongoing learning through hands-on projects, certifications, and security research.