OLUYEDE TOBI STEVEN

JUNIOR CYBERSECURITY PROFESSIONAL | PENETRATION TESTING | DIGITAL FORENSICS

09056937411 | 09037557042 • ooluyede0@gmail.com • Oke-Afa, Isolo, Lagos, Nigeria
linkedin.com/in/oluyede-stephen-tobi • github.com/Cy63rDrift

PROFESSIONAL SUMMARY

Early-career cybersecurity professional with training and internship exposure in ethical hacking, web application and API penetration testing, red teaming, network security, and digital forensics. Familiar with security assessment concepts, network traffic analysis, vulnerability identification, digital evidence preservation, hashing, and forensic documentation through structured training and hands-on laboratory exercises. Holds a B.Sc. in Economics and seeks junior opportunities in cybersecurity analysis, penetration testing, application security, and digital forensics.

EDUCATION

NATIONAL OPEN UNIVERSITY OF NIGERIA (NOUN) — Bachelor of Science (B.Sc.) in Economics | Graduated 2025

CORE COMPETENCIES

Cybersecurity: Ethical hacking fundamentals; web application penetration testing; API security testing; red-team concepts; network security fundamentals; vulnerability assessment; OWASP Top 10 concepts.

Digital forensics: Evidence preservation; file hashing and integrity verification; browser artefact analysis; network traffic analysis; forensic investigation and reporting.

Programming & databases: SQL, HTML, JavaScript, PHP, Go (Golang), C++, and basic Python.

INTERNSHIP EXPERIENCE

SARDONYX TECHNOLOGIES — Ethical Hacking & Web Penetration Testing Intern

January–June 2026 | 6 months | Hybrid

- Completed internship training focused on ethical hacking and web application penetration-testing concepts.
- Built practical familiarity with web security assessment methods and vulnerability identification.
- Developed foundational knowledge of networking for cybersecurity and how network concepts support security testing.

CYBERSTAR — Red Teaming Intern

February–April 2026 | 3 months | Remote

- Received internship exposure to red-team operations and offensive-security methodologies.
- Developed an understanding of adversary simulation, security assessment, and evaluation of defensive controls.

TRAINING & PROFESSIONAL DEVELOPMENT

International Cybersecurity and Digital Forensics Academy (ICDFA) — Web Penetration Testing and Digital Forensics.

Codar Tech Africa — Ethical Hacking and Cybersecurity.

APIsec — API Penetration Testing.

Sardonyx Technologies — Basic Networking for Cybersecurity.

TOOLS & TECHNOLOGIES

Network analysis & reconnaissance: Wireshark, Nmap, Netcat, Amass.

Web & API security: Burp Suite, OWASP ZAP, Postman, OWASP Juice Shop.

Digital forensics: Autopsy, The Sleuth Kit.

OSINT & information gathering: PhoneInfoga, BuiltWith.

Steganography: Steghide, StegSeek.

Development & environments: Kali Linux, Linux, Docker, Git, GitHub, XAMPP.

Tool list reflects technologies used or encountered in training and laboratory work; proficiency varies by tool.

PRACTICAL LABS & PROJECTS

- Performed controlled web application security exercises using OWASP Juice Shop and penetration-testing tools.
- Analysed network traffic and protocol activity using Wireshark in digital-forensics laboratory exercises.
- Practised forensic evidence handling, hashing, integrity checks, and documentation.
- Worked with browser history artefacts and file-system investigation concepts.
- Completed guided cybersecurity learning exercises through Hack The Box and TryHackMe.

• Maintained practical learning notes and project work using Git and GitHub.

ADDITIONAL SKILLS & CAREER INTERESTS

Analytical thinking; research and investigative skills; problem-solving; technical documentation; Microsoft Word, Excel, and PowerPoint; foundational Python programming.

Career interests: Junior Cybersecurity Analyst • SOC Analyst • Junior Penetration Tester • Digital Forensics Trainee • API / Application Security

PROFESSIONAL REFERENCES

Okure Daniel — 08027308127

Oluyede Yetunde — 09052501597