OLARINDE OYEWOLE TIMOTHY

Junior Penetration Tester | Red Team Associate | Cybersecurity Instructor

23B, Dickson Akinwole Street, Off Alakia-Isebo Road, Ibadan, Oyo State, Nigeria

(+234) 904-5502-451, (+234) 913-8871-569 | oyewoleolarinde@gmail.com |
GitHub: https://github.com/Douglas-sama |
Instagram: https://www.instagram.com/cy63r_p0p3/ |
Tiktok: https://www.tiktok.com/@cy63r_p0p3
LinkedIn: www.linkedin.com/in/oyewole-olarinde-cyberpope

Professional Summary

Results-driven cybersecurity professional specializing in penetration testing, red team operations, network security, and security automation. CompTIA Network+, ISC2 Certified in Cybersecurity, and Certified Cybersecurity Educator Professional (CCEP) with hands-on experience across SOC, CERT, OSINT, and enterprise network environments. Proven ability to conduct black-box and gray-box security assessments, automate reconnaissance and exploitation workflows, and produce actionable vulnerability reports aligned with OWASP, MITRE ATT&CK, and NIST standards. Strong background in cybersecurity training, capture-the-flag competitions, and secure software development.

Core Competencies

Penetration Testing • Red Teaming • Network Security • Vulnerability Assessment

Web Application Security • Network Exploitation • Threat Simulation

Incident Response Support • Security Automation • Technical Reporting

OWASP Top 10 • MITRE ATT&CK • NIST SP 800-115 • CVSS

TCP/IP • Subnetting • Firewalls • SIEM • Linux Security

Education

Bachelor of Science (BSc) – Cybersecurity

Abiola Ajimobi Technical University, Ibadan

Professional Experience

Technical Graduate Trainee

TigerLogic Africa | Lagos, Nigeria | March 2025 — Present

- Participating in technical training and development programs across cybersecurity domains
- Supporting enterprise security operations and infrastructure projects.

Freelance Penetration Tester & Security Consultant

Jan 2025 – Present

- Perform black-box and gray-box penetration testing on web applications and internal networks.
- Execute reconnaissance, enumeration, exploitation, and post-exploitation phases using Nmap, Burp Suite, Metasploit, Nessus, and OpenVAS.
- Identify and validate OWASP Top 10 vulnerabilities including authentication flaws, access control issues, injection attacks, and security misconfigurations.
- Conduct network security assessments covering firewall rules, segmentation, exposed services, and insecure protocols.
- Produce technical and executive vulnerability reports with CVSS scoring and remediation recommendations.
- Support clients with security awareness training and risk mitigation guidance..

SIWES Intern – Directorate of Cyber Security (D CYBER)

Defence Space Administration (DSA) | Abuja, Nigeria | June 2024 – December 2024

- Rotated across SOC, CERT, OSINT, and Networking units within a government cybersecurity environment.
- Assisted with incident response support, log analysis, and threat intelligence correlation.
- Supported vulnerability scanning and simulated attacks using Metasploit and Wireshark.
- Participated in network security monitoring, risk assessment, and security posture evaluation.
- Worked with senior analysts on enterprise network defense and threat mitigation activities.

Founder & Technical Lead

CyberCathedral – Campus Cybersecurity Community | 2025 – Present

- Founded and lead a campus-based cybersecurity community focused on hands-on security learning.

- Organize workshops, ethical hacking labs, OSINT sessions, and cybersecurity awareness programs.
- Mentor students in penetration testing, digital forensics, and threat analysis.
- Promote open-source collaboration and cybersecurity skill development.

Cybersecurity Content Creator

CyberPope | Tiktok & Instagram | 2024 – Present

- Develop educational cybersecurity content covering penetration testing labs, attack techniques, and security concepts.
- Create step-by-step walkthroughs based on TryHackMe and Hack The Box platforms.
- Translate complex cybersecurity topics into practical, beginner-friendly learning resources.

Projects

PEN-T Framework | 2025 – Present

- Designed and developed a full-stack penetration testing framework using Django (REST API) and TypeScript/React.
- Implements Role-Based Access Control (RBAC) for Admin, Pentester, Viewer, and Guest roles.
- Modular design covering reconnaissance, scanning, exploitation, and reporting.
- Aligned with OWASP and MITRE ATT&CK methodologies.
- Supports future integration with Metasploit RPC API for automated exploitation.

OSINT Recon Automation Script | 2024

- Built a Python-based OSINT automation tool integrating Shodan, WHOIS, and Sublist3r APIs.
- Automates passive reconnaissance and subdomain enumeration.
- Generates structured JSON and HTML security reports..

Skills

Technical Skills

Networking & Infrastructure (CompTIA Network+)

- TCP/IP, OSI model, and network protocols
- IPv4/IPv6 addressing, subnetting, CIDR
- LAN, WAN, VLANs, routing and switching

- DNS, DHCP, NAT, ARP, ICMP
- Wireless security (802.11, WPA2/WPA3)
- Firewall configuration, ACLs, segmentation
- Network monitoring, troubleshooting, and hardening
- High availability, redundancy, and fault tolerance

Offensive Security

- Web and network penetration testing
- Vulnerability assessment and exploitation
- Post-exploitation and privilege escalation
- Threat modeling and attack simulation
- OWASP Top 10, MITRE ATT&CK, NIST SP 800-115

Programming & Automation

- Python (advanced), Bash
- TypeScript, JavaScript
- Django REST Framework, React.js
- Git/GitHub, Secure SDLC
- Docker (intermediate)

Tools & Platforms

- Metasploit, Burp Suite
- Nmap, Nessus, OpenVAS
- Wireshark, Cisco Packet Tracer
- Linux (Kali, Parrot), Windows Server
- SIEM: Splunk, Graylog

- OSINT: Maltego, Shodan

Soft Skills: Analytical Thinking • Problem Solving • Technical Documentation • Collaboration • Knowledge Sharing • Leadership

Certifications

- CompTIA Network+ (N10-009) – Valid through 2029
- ISC2 Certified in Cybersecurity (CC) – 2025–2028
- Certified Cybersecurity Educator Professional (CCEP) – Red Team Leaders, 2025
- Certified Red Team Operations Management (CRTOM) – Red Team Leaders, 2026
- Cisco Networking Academy – Introduction to Cybersecurity, 2025
- APTECH – Certified Python Programmer, 2021

Competitions & Challenges

- Hck4G CTF 2025 – 60-hour competition
- NITDA x SecDojo CTF 2025 – Top 15%
- ECOWAS x SecDojo CTF 2024 – Top 10%
- TryHackMe Red Team Path – Active participant.

Professional Interests

Penetration Testing • Red Team Operations • Network Security
Security Automation • OSINT & Threat Intelligence
Open-Source Security Tools • Cybersecurity Education

References

Available upon request.