OBIOMA FELICITY UZOH

obiomafelicityuzoh@gmail.com | LinkedIn: *https://www.linkedin.com/in/felicityuzoh* | GitHub: *https://github.com/TechOunik*

PROFESSIONAL SUMMARY

Results-oriented Cybersecurity Analyst and final-year student with hands-on experience in penetration testing, threat analysis, and security monitoring. Proven ability to analyze 500+ packet captures for anomaly detection and author comprehensive vulnerability reports based on OWASP standards. Strong analytical thinker with a solid foundation in offensive security tools (Kali Linux, Metasploit) and defensive frameworks. Serving as a Hackviser Student Ambassador with a commitment to simplifying complex technical concepts for diverse audiences.

TECHNICAL SKILLS

- **Security Assessment:** Penetration Testing, Vulnerability Scanning, Threat Analysis, OWASP Top 10, Risk Assessment.
- **Network Security:** TCP/IP, Wireshark (Packet Analysis), Intrusion Detection, Cryptography, Identity & Access Management (IAM).
- **Tools & OS:** Kali Linux, Metasploit, Nmap, Burp Suite, VMware, Command-Line Interfaces (CLI).
- **Programming & Scripting:** Python (Intermediate), Bash Scripting.

PROJECTS AND PRACTICAL EXPERIENCE

Integrated Security Portfolio (Red & Blue Team Operations) *Self-Directed* | *CAPT & Google Cybersecurity Programs*

- **Vulnerability Assessment (Red Team):** Executed full-lifecycle penetration tests on target virtual machines using **Kali Linux**, **Metasploit**, and **Nmap**, successfully identifying privilege escalation paths and web vulnerabilities (SQLi, XSS).
- **Network Traffic Analysis:** Analyzed **500+ packet captures** using **Wireshark** to detect anomalies and trace simulated brute-force attacks within a virtualized lab.
- **Incident Response (Blue Team):** Performed log analysis and threat detection simulations using **SIEM tools**, **Python**, and **SQL** to investigate security breaches and refine incident response playbooks.
- **Security Reporting:** Authored professional technical reports detailing **12 critical vulnerabilities**, including risk severity ratings and remediation steps aligned with **OWASP Top 10** standards.

- **Lab Configuration:** Built and configured isolated virtual environments in **VMware** to safely simulate attack vectors and audit Identity & Access Management (IAM) controls.

EDUCATION

Bachelor of Science in Cybersecurity *[Miva Open University], [Abuja, Nigeria] Expected Graduation: [May, 2026]*

- **Relevant Coursework:** Network Security, Penetration Testing, Digital Forensics, Intrusion Detection, Security Governance.

CERTIFICATIONS

- **Certified Associate Penetration Tester (CAPT)** – Hackviser | *November, 2025*
- **Google Cybersecurity Professional Certificate** – Coursera | *November, 2025*
- **CompTIA Security+ (SY0-701)** | *In Progress (Target Completion: March 2026)*

LEADERSHIP & VOLUNTEERING

Student Ambassador | *Hackviser October, 2025 – Present*

- Actively engaged with the cybersecurity community to promote ethical hacking best practices and Hackviser training modules.
- Facilitated peer learning by simplifying complex cybersecurity concepts (such as Privilege Escalation and Cryptography) for fellow students.
- Demonstrated leadership by organizing study groups and providing feedback on platform usability.