

Uchenna Emoka

Phone number: (+234) 9064503602 (Home) | **Email address:** ucemoka7@gmail.com | **LinkedIn:** [Uc Emoka](#) |

Whatsapp Messenger: 09064503602

● ABOUT ME

A skilled & dedicated IT professional with hands-on experience as an IT Support Intern, a cybersecurity trainer and a strong passion for cybersecurity. Proficient in troubleshooting, vulnerability analysis, and network security, I continuously enhance my expertise in ethical hacking, pentesting, and security auditing tools.

With solid command-line proficiency and a solution-driven mindset, I excel at identifying and mitigating threats. Strengths include problem-solving, attention to detail, and adaptability, enabling me to contribute effectively to secure and resilient technological environments.

● EDUCATION AND TRAINING

2019/12/16 – 2024/03/29 Enugu, Nigeria
BSC COMPUTER SCIENCE University of Nigeria, Nsukka

- Computer Programming (Python, JavaScript fundamentals)
- Software Development and Software Engineering Principles
- Object-Oriented Programming (OOP)
- Operating Systems
- Computer Networks and Network Administration
- Cybersecurity and Information Security
- Web Development (HTML, CSS, JavaScript)
- Mobile Application Development Fundamentals
- Computer Architecture and Organization
- Problem Solving, Critical Thinking, and Analytical Skills
- Research Methods and Technical Documentation

Website www.unn.edu.ng | **Level in EQF** EQF level 6

● WORK EXPERIENCE

IT SUPPORT TECHNICIAN – C & I LEASING PLC – 2023/04/30 – 2024/06/19 – LAGOS, NIGERIA

Department: IT Department | **Email:** info@c-ileasing.com | **Website:** <https://www.c-ileasing.com/>

- Technical Assistance and Troubleshooting
- set up and configure new workstations, laptops, and mobile devices.
- Performed routine maintenance and upgrades on IT equipment.
- Monitored system performance and network connectivity.
- Assisted with setting up and maintaining servers, printers, and other IT infrastructure.
- Managed user accounts, permissions, and security settings.
- Diagnosed and resolve hardware, software, and network issues.
- Provided remote or in-person support for end-users.
- Installed, configured, and updated operating systems and applications.

CYBERSECURITY TRAINER – DYB AFRICA – 2024/12/11 – 2025/11/14 – LAGOS, NIGERIA

- As a dedicated Cybersecurity Trainer, I've been responsible for equipping individuals with both theoretical foundations and practical, hands-on skills in various cybersecurity domains focusing on the 7 layers of cybersecurity. My focus has been on developing learning experiences that bridge the gap between academic knowledge and real-world application, preparing students for different types of challenges in the digital world and for certifications.

-Designed and facilitated practical labs covering:

- Web Application Penetration Testing using tools like Burp Suite, OWASP Juiceshop, Nikto, etc.
- Network Security and Penetration Testing using Nmap, Metasploit Framework, Wireshark, and Aircrack-ng.
- System Hardening & Vulnerability Assessment with Nessus.

-Created and managed Capture The Flag (CTF) challenges and simulated attacks to reinforce offensive and defensive cybersecurity skills.

-Provided exam preparation support for certifications like **CompTIA Security+**

-Created reusable cybersecurity lab environments using VirtualBox, Kali Linux, Metasploitable, DVWA, and TryHackMe, Blueteamonline, Letsdefend platforms.

APPLICATION SUPPORT SPECIALIST – SCANSOLVE INC – 2025/11/17 – Current – ST JOHNS'S, NEWFOUNDLAND AND LABRADOR, CANADA

- Provided technical support to users by diagnosing and resolving application-related issues.
- Assisted customers with account access, application functionality, and troubleshooting.
- Investigated reported bugs and collaborated with the development team to facilitate timely resolution.
- Documented incidents and maintained accurate support records.
- Guided users through product features and best practices to improve user experience.
- Ensured prompt resolution of customer inquiries while maintaining high service quality.

● **SKILLS**

Programming: Python | Cybersecurity | Tools used (nmap, curl, testssl, nikto, burpsuite, Wireshark, ping, traceroute, nslookup) | Endpoint Security | Linux | Windows | Vulnerability Management | creativity and problem solving | OSINT | Tenable Nessus | Cyber Threat Intelligence | Microsoft Office | System Administration | Network Security Monitoring | Vulnerability Assessment | Web Application Security | Computer Network and Network Security | Kali Linux | I.T. Troubleshooting | Desktop support | Kali Linux, Burp Suite, Metasploit, Wireshark, Nmap, Mimikatz | Good command of Linux OS command line | Active Directory | IT Support | Hardware & Software Support | IT Security | Penetration Testing | Incident Response | Network Security | Technical Support | Python | solve ICT system problems | support ICT system users | manage schedule of tasks

Interpersonal skills

Attention to Details | Core Problem Solving | Computer Literacy,Mangement,Responsibility | Ability To Work Underpressure | Communicative and interpersonal skills | Patience and empathy | Analytical & Research Skills | High Emotional Intelliegnce | Adaptable, organized, goal-oriented, willing to learn | Ability to work in a team and autonomously | Social skills (Adaptable and flexible; sociable; teamwork; high work ethic) | Collaborative Ability | guarantee customer satisfaction | communicate with customers

● **LANGUAGE SKILLS**

Mother tongue(s): **IGBO**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C2	C2	C2	C2	C2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

● **PROJECTS**

2024/02/29 – 2024/03/31

Fraud Prevention Using MFA

This project aims to detect and prevent fraud based on users answers to personal questions asked for Multi-Factor Authentication. Before a user can withdraw money the system has to ensure its the right owner of the account by asking mulple personal questions to the user.

Link https://www.linkedin.com/posts/uc-e-1b36971bb_a-video-of-how-the-bank-application-works-activity-7289699247061454849-lnj-?utm_source=share&utm_medium=member_desktop&rcm=ACoAADMuQVcBy3sXMfko1IunReLLSFVLeElhWKS

OWASP juice-shop & CTFs

I've been testing and practicing my pentesting skills using owasp juiceshop, a vulnerable web application to identify and exploit common web application vulnerbailities based on the OWASP top 10
I've also been testing my skills with vulnerable virtual machines on my virtual box, starting from recon, to scanning, to gaining access and maintaining that access and covering my tracks. This has mostly taught me how to safeguard systems, different attack types and their defence.