

MICHAEL EHONDOR

OFFENSIVE SECURITY, AI RED-TEAMING

08086369667 | ehondormichael14@gmail.com | Lagos, Nigeria
[linkedin.com/in/michael-ehondor](https://www.linkedin.com/in/michael-ehondor) | github.com/McEndo | mcendo.dev

PROFESSIONAL SUMMARY

Offensive security practitioner with hands-on experience in web application penetration testing, access control and authentication vulnerabilities, and agentic-AI red-teaming through labs, CTF challenges, and self-built tooling. Completed the TryHackMe Web Application Pentesting, Jr Penetration Tester, and Cyber Security 101 paths, and built EndoScan, a concurrent Python TCP scanner. Also work as an AI evaluator, reviewing model outputs for technical accuracy, subtle errors, and unsafe content. Work only within authorized scope and document findings clearly.

EXPERIENCE

Cybersecurity Intern

Sep 2024 – Nov 2024

Lagos State Ministry of Innovation and Science and Technology · Lagos, Nigeria

- Explored network reconnaissance and port scanning using Nmap in practical cybersecurity exercises.
- Applied Linux commands and networking fundamentals to understand system operations, network communication, and security concepts.
- Used Python for technical learning and scripting exercises related to cybersecurity.
- Completed hands-on TryHackMe labs covering networking and foundational cybersecurity concepts

IT Intern

Aug 2025 – Oct 2025

Gannetcity Technologies · Lagos, Nigeria

- Supported the development of educational content for the company's IT training initiative, Infotech.
- Organized technical information into structured lesson notes and PowerPoint presentations.
- Conducted independent cybersecurity study alongside assigned responsibilities, strengthening knowledge of Linux, networking, and web security through practical exercises

AI Data Annotator / Evaluator

September 2025 – Present

Mindrift · Remote

- Evaluate AI-generated responses against project rubrics, scoring for accuracy, relevance, completeness, instruction-following, tone and safety
- Compare multiple model outputs side by side, rank them, and write short justifications explaining why one response is stronger
- Fact-check claims in model outputs and flag hallucinations, reasoning errors and unsupported statements
- Identify unsafe, biased or policy-violating content and label it according to the guidelines
- Apply detailed, sometimes changing guidelines consistently across large batches of tasks while keeping quality high

PROJECTS

ARKX / BLEND — Agentic-AI Red-Team Challenges

Technologies: Prompt Injection, System Prompt Leakage, Tool Misuse, Unsafe Eval, MCP/SSE

- Worked through agentic-AI red-team challenges (Bad Robot, Master of Resources, Blind Network Ninja, Shapeshifter), testing AI agents for prompt injection, system prompt leakage, tool misuse, unsafe eval, and MCP/SSE weaknesses in authorized challenge environments
- Submitted a consolidated write-up report covering the challenges

EndoScan — Python TCP Port Scanner

<https://github.com/McEndo/endoscan>

Developed a concurrent TCP Connect port scanner in Python for authorized network security testing. Supports IPv4 addresses and hostnames, custom port lists and ranges, configurable timeouts and worker counts, and clear classification of scan results as OPEN, CLOSED, TIMEOUT, or ERROR. Implemented input validation, scan summaries, and automated unit tests. Benchmarked concurrent scanning to evaluate performance improvements across different worker counts.

Web Application Security Testing Practice

Technologies: Burp Suite, HTTP, Web Application Security, PortSwigger Web Security Academy

Practiced identifying and analyzing web application vulnerabilities in authorized training labs. Focused on access control weaknesses, authentication and authorization behavior, HTTP request manipulation, and understanding how applications enforce security restrictions.

Security Write-ups and Endo Field Notes

<https://github.com/McEndo/WriteUps> | <https://mcendo.dev>

Technologies: Web Development, Technical Documentation, Cybersecurity Research

Maintain a GitHub write-ups repository and a personal cybersecurity website and field-notes project to organize technical learning, document security concepts, and maintain practical cybersecurity knowledge. Focused on building a structured resource for recording research and documenting web application security testing techniques.

EDUCATION

Bsc in Computer Science

Lagos State University of Science and Technology

2022 – 2026

CERTIFICATIONS

Web Application Pentesting — TryHackMe

29 Nov 2025

Jr Penetration Tester — TryHackMe

24 Oct 2025

Cyber Security 101 — TryHackMe

12 Sep 2025

SKILLS

Offensive Security: Web Application Security Testing | Penetration Testing Fundamentals | Web Application Enumeration | Access Control Vulnerability Analysis | Authentication Testing | Authorization Testing | HTTP Request and Response Analysis | Vulnerability Identification | XSS | SQLi | SSRF | CSRF | OAuth Vulnerabilities | Linux Privilege Escalation | Network Scanning | TCP Connect Port Scanning | DNS Resolution

AI Security and Evaluation: Agentic-AI Red-Teaming | Prompt Injection | System Prompt Leakage | AI Model Evaluation | AI-Generated Response Evaluation | Instruction Following Evaluation | Response Accuracy Assessment | Error Identification | Structured Feedback

Tools and Platforms: Kali Linux | Burp Suite | Nmap | PortSwigger Web Security Academy | TryHackMe | Git | GitHub

Development: Python Programming | JavaScript | TypeScript | React | Node.js | Vite | HTML | CSS | Command-Line Interface (CLI) Development | Unit Testing | Software Debugging | Concurrent Programming Fundamentals | CI/CD Workflows

Professional: Technical Documentation | Technical Research | Written Communication | Critical Thinking | Analytical Reasoning | Attention to Detail | Following Complex Instructions | Independent Learning | Time Management

LANGUAGES

English — Native