EDIE SIBANDA

064 089 3160

ediesibanda0010@gmail.com

South Africa | Open to Global Remote

EDUCATION

Fidelitas Comprehensive School
- Matric (Diploma)

Currently
Ongoing self-study in Cybersecurity & IT fundamentals through online labs and practical exercises

LANGUAGES

- English
- Isizulu

SKILLS

- Cyber security skills
- Time Management
- Creativity
- Web design
- Web development
- Critical Thinking
- Problem solving

TECHNICAL SKILLS

- Operating Systems: Linux (WSL), Windows
- Networking & Recon: Nmap scanning, basic enumeration, port forwarding concepts
- Traffic Analysis: Wireshark, tcpdump (basic usage)
- Troubleshooting: ping, curl, netstat, basic system diagnostics
- Scripting & Tools: Bash fundamentals, command-line usage

EDIE SIBANDA

Profile Summary

Entry-level IT & cybersecurity practitioner with hands-on experience in Linux (WSL) and Windows environments. Skilled in basic network reconnaissance, traffic inspection, and system troubleshooting using tools like Nmap, Wireshark, and curl. Comfortable working remotely, documenting findings, and learning through practical labs. Actively building real-world technical skills for IT support and cybersecurity roles.

Remote Work & Support Skills

- Online research and information gathering
- Data entry and document preparation
- Customer communication (email & chat)
- Task organization and follow-through
- Fast typing and efficient tool usage

Cybersecurity & Technical Projects

- Performed network scanning and enumeration labs to identify exposed services and misconfigurations.
- Analyzed HTTP and network traffic using Wireshark to identify anomalies and request flows.
- Practiced secure remote access concepts, tunneling, and basic system hardening.
- Troubleshot Linux and Windows issues related to networking and connectivity
- Practiced identifying common web vulnerabilities such as insecure access control, parameter manipulation, and logic flaws through hands-on labs.
- Analyzed HTTP requests and responses using browser DevTools, Burp Suite, and curl to understand application behavior
- Tested authentication and authorization assumptions by modifying request parameters and replaying requests in controlled lab environments.

I've used **CyberED**, **TryHackMe**, **Hack The Box**, **PortSwigger**