Natachi Ike-Obasi - Resume
Ike-Obasi Natachi Ikechukwu
Email: natachiobasi@gmail.com
GitHub: Natcode01

Professional Summary

Motivated and technically skilled cybersecurity professional with hands-on experience in security engineering, cloud security, and offensive security lab environments. Proficient in identifying and mitigating cloud-based vulnerabilities, particularly in AWS, and actively strengthening expertise in Microsoft Azure and security best practices. Demonstrates a strong foundation in DevSecOps, threat detection, and secure system design. Committed to continuous learning, with a passion for building resilient, secure infrastructure and contributing to modern security teams.

Skills

Technical Skills

Cloud Security: AWS Security, Cloud Penetration Testing, Microsoft Azure

Security Engineering: Network Security, DevSecOps, Security Analysis, Penetration Testing

Platforms & Tools: AWS, Linux, JavaScript, Infrastructure as Code (IaC) basics

Core Competencies

- Cybersecurity Fundamentals

- Security Best Practices

- Vulnerability Management

- Threat Detection

- Problem-Solving

- Team Collaboration

- Attention to Detail

Tools: Nmap, Metasploit, Burp Suite, AWS CLI, MS Sentinel, KQL

Certifications & Training

Attacking and Defending AWS Environments - TryHackMe

DevSecOps – TryHackMe

Security Engineer – TryHackMe

CompTIA Security+ (In Progress)

Defending Azure - TryHackMe

Projects & Hands-On Labs

TryHackMe Labs & Challenges

Basic Pentesting
Performed enumeration, exploitation, and privilege escalation on Linux-based systems.

Tools used: Nmap, Metasploit

Mother's Secret
Investigated hidden credentials and files using CTF-style OSINT and local analysis techniques.

Tools used: Nmap, manual enumeration

CI/CD & Build Security
Hardened DevOps pipelines by identifying misconfigurations and securing build environments.

Tools used: Burp Suite

IAM Permissions (AWS)
Exploited insecure IAM roles and demonstrated privilege escalation paths in AWS.

Tools used: AWS CLI

AWS VPC – Data Exfiltration
Simulated and prevented data exfiltration scenarios via misconfigured VPC setups.

Tools used: AWS CLI

MS Sentinel: Just Looking
Explored security monitoring, analytic rules, and alert investigation through TryHackMe labs.

Tools used: Microsoft Sentinel portal, KQL

Work Experience

Electrical Laboratory Assistant (Intern)
Nnamdi Azikiwe University, Awka
Nov 2022 – May 2023

- Assisted in maintaining and setting up electrical lab equipment for student practical

- Supported instructors during lab sessions to ensure safety compliance and operational efficiency

- Developed technical precision and attention to detail in a hands-on academic environment

Education

B.Eng., Electrical Engineering
Nnamdi Azikiwe University, Awka
Aug 2018 – Dec 2023

Cybersecurity: TryHackMe