NKASIOBI IRENE OKEKE

Entry-Level Penetration Tester

nkasy.irene@gmail.com | +2349064932389 | Awka, Nigeria | linkedin.com/in/nkasiobi-okeke-352735248

Summary

An entry-level penetration tester with strong foundation in ethical hacking and experience in web application testing, penetration testing, vulnerability assessment and report, python scripting, Microsoft suite and network analysis. Skilled in penetration testing tools like burp suite, nikto, nmap, owasp zap, wireshark and others. Currently advancing my penetration testing skills through deployment of DVWA, Bwapp and owaspbwa virtual machine for real world penetration testing. Basic knowledge of IT security and Active Directory. Holds a BSc in Human Physiology.

Professional Experience

Regia Digitals

AI Content Creator **Nov, 2025-Present**

- Image Generation using Google AI studio
- Voice prompt generation using Google AI studio
- Video Generation using various AI tools such as Hygen, lipsync and dizine
- Video editing using capcut and canva
- Report writing

Deltaware Solution Limited

Cybersecurity Intern **June-July, 2025**

- Cryptography and encryption
- Text encryption and decryption using RSA, DES, AES and blowfish algorithms
- Steganography
- Secure chat application and QR code encryption
- python

Digitanotion Limited **March-May, 2025**

Cybersecurity intern (VAPT) Nigeria.

- Performed real world OSINT challenge using tineye and Google hacking
- Setting up home lab for vulnerability assessment and kali Linux commands
- Research assignment on owasp top ten.
- Performed a vulnerability assessment (SQLi, XSS stored and reflected) on an open source web app bWAPP using Nessus and nikto and applied CVSS to score the vulnerabilities found.
- Mentorship on CTFs and bug bounty using Hackerone, Bugcrowd and tryhackme platforms.
- Capstone project challenge on performing a vulnerability assessment and identifying security risks in owasp juice shop.

Hack Secure **Feb-Mar 2025**

Cybersecurity intern (offensive security) India.

- Lab practice on port scanning using Nmap, brute force using Dirb and intercepting a network traffic and finding the login credentials using wireshark.
- Red team fundamentals using tryhackme room and exploring common attacks using tryhackme common attacks room.
- Performed task on CTF with tryhackme picklerick room where stimulated attack like lateral movement and post-exploitation like credential harvesting were performed.
- Password strength determination with python automation.

Education

Nnamdi Azikiwe University **Dec 2023**
Bachelor of Science in Human Physiology. Awka, Nigeria

Certifications and Skills

TCM Practical Helpdesk Support
Desktop computer components and repair, installing, replacing and troubleshooting laptops, operating systems, virtualization, windows, linux, networking, security, remote support, ticketing, windows active directory.

Packt Coursera Ethical Hacking Bootcamp **May, 2025**
Skills: setting up pentest lab, linux and windows command essientials, networking terminology and tools, passive information gathering and footprinting (dig, google, whois, shodan, the harvester), active information gathering and port scanning using zenmap, nmap and nmap SE, web application penetration testing, wireless penetration testing, system hacking and exploitation (metasploit, metasploit modules, SSH brute force using metasploit, meterpreter session, wine installation, privilege escalation, post exploitation attacks, eternalblue exploit), MITM attacks, python basics, developing an advanced backdoor, developing a keylogger, developing a brute force attacker

3MTT Cybersecurity Professional **May, 2024**
Skills: ethical hacking, cybersecurity fundamentals, OSINT, threat and vulnerability management, risk assessment and management, kali linux installation and commands, web application penetration testing, owasp juice shop, burpsuite, owasp zap, metasploit, SIEM (wazuh), networking protocols, cybersecurity tools and laws.

Cisco Certified Ethical Hacker **Dec, 2024**
Skills: ethical hacker, tools and code analysis, reporting and communication, post-exploitation techniques, cloud, mobile and IoT security, social engineering attacks, exploiting wired and wireless network, OSINT, networking basics, cyber laws (SOX, GLBA, PCI DSS), cybersecurity domains(NIST, ISO 27000, CIA, CIS), report writing.

Computer Trainee **Oct, 2016-Mar, 2017**
Skills: Microsoft office suites (excel, word, powerpoint, designer, onenote, access, outlook), command prompt commands, powershell, internet, taskmanager, event viewer, disk partitioning, OSs VM installation, BIOS, knowledge about windows and computer, basic math, data entry, typing, word processing.

Projects

GitHub: https://github.com/Nkasy11