PHILIP MWANGI

Cyber Security Analyst

Nairobi, Kenya • +254719529390 • iamphilipmwangi@gmail.com

Professional Summary

Aspiring cybersecurity specialist with hands-on experience in intrusion detection systems, penetration testing, web application security (OWASP Top 10), and phishing simulations. Skilled in identifying, analyzing, and mitigating security vulnerabilities, with a strong foundation in ethical hacking and network forensics. Seeking a challenging role in a dynamic organization where I can leverage my technical expertise to protect digital assets, enhance security frameworks, and contribute to building resilient cyber defense strategies.

Websites, Portfolios, Profiles

- https://nimwangibana.github.io/mywebsite/
- https://github.com/nimwangibana
- www.linkedin.com/in/mwangiwav

Technical Skills

Cyber security

Intrusion Detection Systems (IDS), Network traffic analysis, Web application penetration testing, OWASP Top 10 testing, Phishing simulations and credential harvesting, Offensive & defensive security, Network security fundamentals.

Education

- **Diploma in Cybersecurity and Ethical Hacking** - Institute of Software Technologies January 2025 - February 2026
- **Certificate in Cybersecurity and Ethical Hacking-** Institute of Software Technologies May 2024 - September 2025
- **High School Certificate** - UpperHill School January 2020 - November 2023

CyberSecurity Projects

1. **Intrusion Detection Systems (IDS) Implementation**

- Designed, configured, and deployed Snort IDS to monitor and analyze network traffic in real-time.
- Created custom detection rules to identify and respond to malicious activities such as ICMP floods, SSH brute force attempts, and other network attacks.
- Conducted forensic analysis using Wireshark and Snort logs to document attack patterns, network anomalies, and provide actionable insights.

2. **OWASP Top 10 Web Vulnerability Assessment**

- Performed comprehensive web application security assessments targeting vulnerabilities listed in the OWASP Top 10, including SQL injection, XSS, insecure authentication, and sensitive data exposure.
- Utilized tools and manual testing techniques to identify, exploit, and document security weaknesses.
- Provided mitigation recommendations to strengthen web application security posture.

3. **Penetration Testing**

- Conducted ethical hacking exercises to simulate real-world cyberattacks on web applications and network environments.
- Used reconnaissance, scanning, exploitation, and post-exploitation methodologies to identify security gaps.
- Compiled detailed penetration testing reports including risk assessments, vulnerabilities discovered, and remediation strategies.

4. **Phishing Simulation and Security Awareness**

- Implemented phishing campaigns using GoPhish to test and evaluate end-user susceptibility to social engineering attacks.
- Developed customized email templates and landing pages to simulate realistic phishing scenarios.
- Analyzed click-through and credential submission data to measure effectiveness and educate users on phishing risks.

Languages

- **English:** Full Professional proficiency
- **Swahili:** Full Professional proficiency

Professional Attributes

- Strong analytical and problem-solving skills
- Detail-oriented and methodical in investigations
- Quick learner, adaptable to new technologies
- Effective communicator and team player