EMMANUEL KIBET KORIR

Cybersecurity Engineer | Full-Stack Developer | ML Specialist

Email: ekorir555@gmail.com | GitHub: github.com/Korir555 | Portfolio: korir555.github.io/cybersecurity-portfolio

Nairobi, Kenya | Open to Remote and Freelance Opportunities

PROFESSIONAL SUMMARY

Cybersecurity engineer with expertise in penetration testing, threat detection, machine learning, and enterprise security. Demonstrated ability to design and deploy production-grade security applications across network, application, ML, and compliance domains. Portfolio includes 15 professional cybersecurity projects totaling 15,000+ lines of code. Strong background in Python, Flask, React, scikit-learn, cryptography, and secure coding practices.

TECHNICAL SKILLS

Security: Penetration Testing, Threat Detection, Cryptography (AES-256, RSA, HMAC), Incident Response, MITRE ATT&CK; Framework, OWASP Top 10, Vulnerability Assessment, Network Security, Secure Coding, SSL/TLS, DNS Security, DNSSEC

Machine Learning: scikit-learn, Random Forest, Gradient Boosting, Feature Engineering, Anomaly Detection, Classification, Cross-Validation, ROC-AUC, Model Evaluation, pandas, numpy

Languages: Python, JavaScript, Bash, SQL

Backend: Flask, FastAPI, Node.js, Express.js, RESTful API Design

Frontend: React, HTML/CSS, Responsive Design, Dark Theme UI/UX

Databases: SQLite, PostgreSQL

Tools & Platforms: Git, Docker, Kali Linux, Nmap, Burp Suite, Metasploit, dnspython, BeautifulSoup, cryptography library

PROFESSIONAL EXPERIENCE

Cybersecurity & ML Portfolio Developer (Freelance) | Nairobi, Kenya | 2024 - Present

Designed, developed, and deployed 15 production-grade cybersecurity and machine learning projects spanning network, application, machine learning, and enterprise security domains. Implemented full-stack security applications using Flask, React, and cryptographic libraries. Established comprehensive documentation and GitHub repositories for all projects.

Key Accomplishments:

- Built ML-based Intrusion Detection System with 95%+ accuracy using Random Forest and Gradient Boosting classifiers
- Developed Web Application Security Scanner detecting OWASP Top 10 vulnerabilities with CVSS scoring
- Created DNS & Certificate Intelligence Tool for network reconnaissance and SSL/TLS analysis
- Implemented Security Audit Dashboard supporting GDPR, HIPAA, PCI-DSS, and ISO27001 compliance frameworks
- Built Phishing Email Detection Model with 94% precision and explainable feature importance
- Implemented cryptographic systems (AES-256, RSA) meeting NIST standards
- Conducted network enumeration and penetration testing against deliberately vulnerable systems

AI/ML Evaluation Specialist (Freelance) | Outlier AI | 2024 - Present

Evaluated large language model outputs and AI system quality. Performed QA on model responses, conducted prompt engineering for edge case analysis, and provided detailed technical feedback on performance and improvement areas.

EDUCATION

Bachelor of Science in Cybersecurity and Digital Forensics | Open University of Kenya | Expected 2028

Relevant Coursework: Threat Modeling (STRIDE, OAuth 2.0), Intrusion Detection Systems (Snort), SQL Injection and Web Vulnerabilities (DVWA), Linux System Enumeration, Penetration Testing, Network Security

PORTFOLIO PROJECTS (15 TOTAL)

Enterprise-Grade Tools (Projects 12-15): ML-based Intrusion Detection System (scikit-learn, 95%+ accuracy) | Web Application Security Scanner (OWASP detection, CVSS scoring) | DNS & Certificate Intelligence Tool (reconnaissance, SSL/TLS analysis) | Security Audit Dashboard (GDPR, HIPAA, PCI-DSS, ISO27001 compliance)

Core Security Tools (Projects 7-11): SOC Incident Response Simulator (30+ MITRE ATT&CK; scenarios) | Phishing Detection Model (94% precision) | Network Enumeration Lab (Kali Linux) | Professional Port Scanner (CVE correlation) | Hybrid File Encryption (AES-256-GCM + RSA)

Penetration Testing Labs (Projects 1-6): Web application security assessments, command injection exploitation, SQL injection, XSS testing, WordPress vulnerability assessment, DVWA analysis

CERTIFICATIONS & ACHIEVEMENTS

- 15 production-grade security applications deployed on GitHub (1000+ lines each)
- Implemented cryptographic systems meeting NIST standards (PBKDF2, AES-256, RSA-2048+, HMAC-SHA256)
- Developed machine learning models with cross-validation and performance optimization (ROC-AUC 0.97+)
- Conducted network reconnaissance and vulnerability assessment on intentionally vulnerable systems
- Built enterprise compliance audit engines (GDPR, HIPAA, PCI-DSS, ISO27001)
- Created comprehensive technical documentation and professional portfolio website
- Demonstrated SQL injection, XSS, command injection, CSRF, and authentication bypass vulnerabilities