MITCHELE JEBET

Cybersecurity Analyst

jebetmichele@gmail.com | +254794658627 | Nairobi, Kenya

LinkedIn: linkedin.com/in/mitchelejebet | GitHub: github.com/Girlweb

Portfolio: mitchele-jebet-cyber-shield.lovable.app

PROFESSIONAL SUMMARY

Cybersecurity enthusiast and Electrical Engineering student with hands-on experience in network security, penetration testing, and DevSecOps practices. Skilled in threat detection, vulnerability assessment, and security automation with proven ability to identify and remediate security risks. Completed 50+ practical security challenges demonstrating expertise in offensive and defensive security techniques.

EDUCATION

Bachelor of Electrical Engineering (In Progress)

Kenyatta University, Nairobi | Expected Graduation: 2026

Cybersecurity Training Program | Moringa School | 2024

Professional Foundations Certificate | ALX Africa | 2020

TECHNICAL SKILLS

Security Tools: Wireshark, Burp Suite, Metasploit, Nmap, Kali Linux, Nessus, OpenVAS, SQLMap, Hydra, John the Ripper, Hashcat, Nikto, Gobuster, Aircrack-ng

SIEM & Monitoring: Wazuh, Splunk, Security Onion, ELK Stack, Suricata, OSSEC

Network Security: Cisco networking, VPN configuration, firewall management, IDS/IPS, network traffic analysis

Penetration Testing: Web application testing, vulnerability assessment, exploit development, security auditing

DevSecOps: Docker, Jenkins, GitLab CI, GitHub Actions, Terraform, Ansible, CI/CD pipeline security

Programming: Python, Bash scripting, PowerShell

Data Formats: JSON, XML, YAML - security configuration and log analysis

Operating Systems: Ubuntu, Kali Linux, Parrot OS, Windows Server, Red Hat Enterprise

PROJECTS

DevSecOps Pipeline Assessor | Ongoing

GitHub: github.com/Girlweb/devsecops-pipeline-assessor

Developing comprehensive security assessment tool for CI/CD pipeline vulnerability detection

Implementing automated security scanning integrated with GitLab CI and Jenkins pipelines

Utilizing Docker for containerized security testing environments ensuring consistency

Applying Infrastructure as Code principles with Terraform for reproducible security configurations

Integrating SonarQube for continuous code quality and security analysis

Medical IoT Security Simulation Tool | 2024

Engineered security testing framework simulating attack vectors against medical IoT devices

Conducted network traffic analysis using Wireshark and MQTT protocol inspection

Identified vulnerabilities specific to healthcare environments ensuring HIPAA compliance requirements

Performed systematic penetration testing and documented findings with remediation recommendations

Demonstrated understanding of sector-specific security requirements and regulatory frameworks

AI Data Annotation & Quality Assessment Tool | 2024

GitHub: github.com/Girlweb/ai-data-annotation-tool

Developed Python-based tool with security-focused data validation and integrity checking

Implemented secure data processing pipelines handling sensitive training datasets

Applied security best practices including input validation, sanitization, and access controls

Generated audit trails and compliance reports in JSON/CSV formats

Web Application Penetration Testing | 2024

Completed advanced PortSwigger Web Security Academy labs covering OWASP Top 10 vulnerabilities

Successfully identified and exploited SQL injection, XSS, CSRF, and authentication bypass vulnerabilities

Conducted security assessments using Burp Suite, OWASP ZAP, Nikto, and custom Python scripts

Documented findings with detailed technical reports including proof-of-concept exploits and remediation guidance

Network Security Implementation | 2023

Designed and configured secure network infrastructure using Cisco equipment and protocols

Implemented firewall rules, VLANs, access control lists, and VPN tunnels

Conducted network hardening and security baseline configuration

Achieved 95% security compliance score in academic security audit

PRACTICAL EXPERIENCE

Cybersecurity Challenge Platforms | 2023 - Present

Completed 50+ hands-on security challenges on TryHackMe and HackTheBox platforms

Ranked in top 15% of active TryHackMe users demonstrating consistent performance

Practical experience with penetration testing methodologies, privilege escalation, and post-exploitation

Developed systematic approach to security assessments and vulnerability remediation

Documented findings and created detailed write-ups of security challenge solutions

CERTIFICATIONS

Cisco Certified Network Associate (CCNA) | Cisco Networking Academy | 2023

Pre Security Learning Path | TryHackMe | 2024 | Certificate: THM-850TRUZ5A3

ArcX CTI - Cyber Threat Intelligence | ArcX | 2024

Endpoint Security Badge | Cisco Networking Academy | 2024

Initial Configuration of Network Devices Badge | Cisco Networking Academy | 2024

RELEVANT QUALIFICATIONS

Strong analytical and problem-solving skills with systematic approach to security challenges

Attention to detail essential for identifying security vulnerabilities and configuration weaknesses

Experience with security documentation, technical report writing, and presenting findings

Comfortable working independently and collaboratively in remote team environments

Quick learner who stays current with emerging threats and security technologies

Passionate about cybersecurity career path with commitment to continuous learning

LANGUAGES

English (Fluent) | Swahili (Native) | French (Intermediate)

AVAILABILITY

Available for internship/entry-level positions with flexible scheduling

Can commit to full-time or part-time arrangements depending on role requirements