

Joshua Maina

IT Practitioner | Cybersecurity Technician

✉ joshuamaina83@gmail.com

☎ +254-790-611760

🌐 www.JoshuaMaina.com

I am a 22-year-old student currently enrolled in a Bachelor of Science program in Information Technology at KCA University Campus in Nairobi, Kenya and my passion lies in the field of Information Technology and Cybersecurity. I am currently undertaking a three-month internship as a Security Analyst, where I am gaining practical experience and deepening my understanding of these fields. My ultimate goal is to become an expert in IT and cybersecurity, and I am actively seeking job opportunities that will allow me to apply my skills, continue learning, and contribute to the security of information systems.

Experience

Partnership for Economic Policy - Research Assistant and Data Collector *October 2022 - May 2023*

- Took an training program under contract to learn about data collection and research work sponsored by Partnership for Economic Policy a Non Government Organization for Research studies
- Coordinated data collection efforts, including designing data collection methods, gathering relevant information from various sources, and ensuring data accuracy and integrity.
- Demonstrated strong communication and interpersonal skills while conducting interviews when collecting data.
- Adapted quickly to changing project requirements and priorities, demonstrating flexibility and resilience in navigating complex research environments

CloudFactory - Data Annotator (Part-Time) *May 2023 - Present*

- Completed comprehensive training programs focused on data annotation using tools such as Expensify.
- Received hands-on instruction and coaching from experienced trainers and subject matter experts, gaining insights into best practices and industry standards for data annotation.
- Participated in practical exercises and simulated annotation tasks to reinforce learning objectives and enhance annotation skills.
- Successfully completed assessments and evaluations to validate competency in data annotation techniques and quality control procedures

Foresight Tech Group - Security Analyst Intern *May 2024 - Present*

- Received training and guidance on how to implement SSH Configurations on a Virtual Private Server
- Successfully completed training in the implementation of host-based firewalls, gaining hands-on experience in configuring and managing firewall software on individual devices.
- Participated in a comprehensive training program focused on implementing SSH configurations on Virtual Private Servers (VPS), under the guidance of experienced professionals.
- Acquired hands-on experience in configuring Secure Shell (SSH) settings to enhance security and access control on VPS instances.
- Developed proficiency in managing SSH keys, configuring SSH access restrictions, and implementing best practices for securing remote server access.

Education

<div><div></div><div>Consolata High School</div></div> <div><ul style="list-style-type: none">• Active in Sports (Soccer)• Active in Computer Club</div>	2017-2019
<div><div></div><div>KCA University</div></div> <div><ul style="list-style-type: none">• Bachelor of Science, Information Technology</div>	2020-2024

Certifications

- EC-Council Certified Cybersecurity Technician (CCT)
- Cisco Network CyberOps Associate
- Certification in Graphic Design (Photoshop, InDesign, Illustrator, Canva)

Technical Skills

Programming Languages: Python, C++, JavaScript, SQL, Google Firebase

- Proficient in Python programming language for software development and scripting tasks

Web Development

- Proficient in HTML ,CSS and JavaScript
- Developed web applications using HTML ,CSS and JavaScript intergated with AI Components

Database Management

- Proficient in leveraging Google Firebase for backend services and cloud infrastructure. Experienced in using Firebase Authentication for user authentication and authorization
- Google Firebase for cloud store and Web App deployments
- Proficient in creating and managing databases using Microsoft Access. Knowledge in designing relational databases, creating tables, queries, forms, and reports
- SQL Knowledge in writing and optimizing SQL queries to retrieve, manipulate, and analyze data from relational databases and stored procedures. Performing data manipulation tasks such as inserting, updating, and deleting records, as well as transforming data using functions and expressions.

Installation and Usage of Operating Systems (Windows and Linux)

- Proficient in installing and configuring various versions of Windows operating systems.
- Skilled in troubleshooting common Windows issues, performing software installations, and managing user accounts and permissions
- Comfortable with using Windows administrative tools and utilities for system monitoring, performance tuning, and security management
- Proficient in installing and configuring different distributions of Linux such as Ubuntu, CentOS
- Knowledge in using the Linux command-line interface (CLI) for system administration tasks including package management, file system operations, and user management

CyberSecurity

Skills

Administrative Controls

- Windows Group Policy Management: Familiar with implementing strong password policies and enhancing security using Windows Group Policy.
- Auditing Policy Implementation: Exposed to enhancing accountability and compliance by implementing auditing policies to track user activities.
- Secure Network Policy Development: Familiar with developing and implementing policies to safeguard network infrastructure and sensitive data.

Network Logs and Monitoring

- Intercepting Network Traffic: Proficient in intercepting network traffic using Wireshark and tcpdump for detailed analysis and troubleshooting.
- Applying Filters in Wireshark: Knowledgeable in applying various filters in Wireshark to streamline network traffic analysis and focus on specific packets or protocols.
- Network Scanning: Capable of scanning networks to identify hosts in the local network, facilitating network inventory management and security assessment using nmap.
- Windows Event Log Configuration: Exposed to configuring, viewing, and analyzing Windows Event Logs to monitor system activities and identify security incidents.

Offensive Security Techniques (Penetration Testing)

- Man-in-the-Middle (MITM) Attack: Exposed performing MITM attacks using Cain & Abel.
- MAC Flooding: Good knowledge in executing MAC flooding attacks using macof.
- Denial of Service (DoS) Attack: Capable of conducting DoS attacks on target hosts using hping3.
- SQL Injection Attack: Familiar with performing SQL injection attacks against MSSQL to extract databases using sqlmap.
- Password Auditing: Familiar in auditing system passwords using John-the-Ripper.
- WPA2 Network Cracking: Familiar with cracking WPA2 networks using Aircrack-ng.

Vulnerability Research and Assessment

- Exposed to extensive data collection through search engines, utilizing advanced search techniques to gather relevant information for threat analysis and intelligence gathering.
- Conducted vulnerability research in Common Weakness Enumeration (CWE), analyzing software and hardware weaknesses to proactively address potential vulnerabilities.

Cryptography

- Hash Calculation: Proficient in HashCalc for data integrity.
- MD5 Hash Calculation: Familiar with MD5 Calculator for verification.
- Data Encryption/Decryption: Exposed to BCTextEncoder for secure transmission/storage.
- Certificate Management: Capable with OpenSSL for secure communication.

Malware Development and Analysis:

- Trojan Creation: Familiar with developing Trojans to gain unauthorized access to target systems.
- Virus Creation: Knowledge in crafting viruses to infect and compromise target systems.
- Worm Creation: Capable of creating worms using tools like Internet Worm Maker Thing for widespread propagation.
- System Monitoring and Surveillance: Familiar in using Spytech SpyAgent for user system monitoring and surveillance.

Intrusion Prevention and Detection

- Firewall Implementation: Familiar in host-based firewall protection using iptables (Linux) and Windows Firewall.
- Network-Based Firewall: Knowledge in deploying pfSense firewall for enhanced security by blocking unwanted website access and insecure ports.
- Intrusion Detection Systems (IDS): Good knowledge in implementing Suricata IDS for real-time threat detection and using Splunk for log analysis to enhance incident response.
- Malicious Traffic Detection: Familiar with HoneyBOT for proactive detection and analysis of malicious network traffic.
- VPN Setup: Capable of establishing secure VPN connections for remote access and data transmission.

Soft Skills

- Communication (Verbal and Written) , Strong communication skills through clear and effective verbal presentations, written documentation, and interpersonal interactions, fostering open dialogue and understanding among team members.
- Proficient in collaborating with teams to achieve common goals, leveraging diverse perspectives and expertise to drive innovation and problem-solving while fostering a supportive and inclusive work environment.
- Adaptable and flexible in response to changing priorities, environments, and circumstances, quickly adjusting strategies and approaches to effectively meet evolving project requirements and organizational needs.
- Paying Attention to Details by exhibiting attention to detail in tasks, documentation, and deliverables, ensuring accuracy, quality, and consistency across all aspects of work to meet or exceed established standards and expectations.

Projects

- Developed an AI-Powered Car Ecommerce Web App using HTML,CSS and JavaScript with Google Firebase as a backend Management Service.
- Built an Nmap-python Network scanner. The script automates the execution of Nmap commands, This project demonstrates the integration of Python scripting with the powerful network scanning capabilities of Nmap on the Kali Linux environment
- Developed a Python-based password cracker utilizes encryption methods to decrypt passwords and gain unauthorized access to protected accounts.
- Built a Python-based file encrypter offers a straightforward solution for securing sensitive data by encrypting files using cryptographic algorithms.
- Set Up a PenTest Lab environment using Kali Linux and Metasploitable for personal PenTest training
- Developed a Phishing Link Scanner used to distinguish between legitimate and fake websites to enhance internet security using Python
- Built a portfolio website using HTML ,JavaScript displaying my skills and aspirations

To view them here is my github profile: <https://github.com/joshmainaa7>

Hobbies

- Football
- Drawing and Art
- Visiting Art Museums
- Reading Novels
- Travelling

References

Mrs.Jacqueline Mumbi Gitau

Delivery Manager

CloudFactory

Email:Jacqueline.mumbi@cloudfactory.com

Mobile No;+254723987496

Contacts/Social Media

Email: joshuamaina83@gmail.com

Phone Number: +254 790611760

Address: 6681-00100 G.P.O Nairobi ,Kenya

LinkedIn: www.linkedin.com/in/joshua-maina-4752a1241

GitHub: <https://github.com/joshmainaa7>