Allan Kariuki Mbugua
Github:https://github.com/ALLann123
Linkedin:https://www.linkedin.com/in/allan-mbugua-58b855344/
Contact: +254723269755
Email: kariukiallan81@gmail.com

EXPERIENCE

IT SUPPORT, JOMO KENYATTA UNIVERSITY (ISS) MAY 2021- AUGUST 2021

Computer Maintenance and troubleshooting • Repairing computer hardware such as printers • Installing new networking devices such as wireless access points, distribution switches, and termination of fiber cables to link buildings. • Network administration of the organization. • Network design tasks such as creating new virtual local area networks (VLANs) in the organization network

EDUCATION

Jomo Kenyatta University of Agriculture and Technology Jan 2023 – present
Nairobi, Kenya
● **BSc Information Technology**

Jomo Kenyatta University of Agriculture and Technology Jan 2020 – June 2022
● **Diploma in Information Technology (Credit)**

CERTIFICATIONS

Certified Cyber Security Analyst **October 2024**

By CyberWarfare labs

Focuses on securing and monitoring the network using tools such as Wireshark, implementing intrusion detection systems (e.g., **Snort**) to detect suspicious activity within the network, and configuring firewalls using **Linux iptables**. The course also covered **web penetration testing**, **Bash** and **PowerShell scripting**, as well as **host exploitation**.

API Security Fundamentals **October 2024**

By APISEC University

Provides foundation knowledge to get started in discovering API endpoints through fuzzing and methods to secure APIs.

PROJECTS

Web Enumeration Script **November 2024**

Automated web application enumeration using Kali Linux tools and Bash scripting. The script performs port scanning, domain information gathering, reverse DNS, subdomain enumeration, directory brute-forcing, screenshot capture of the subdomains discovered for faster analysis, and historical file analysis with the Wayback Machine.
Configured to run via cron jobs for continuous reconnaissance.

ARP Detection **December 2024**

The Python Scapy library is a powerful packet manipulation tool. It enables attacks such as ARP spoofing (for man-in-the-middle attacks) and DHCP starvation on switches. I wrote a tool to detect ARP spoofing in a network by monitoring ARP table changes and sending alerts to prevent man-in-the-middle attacks.

Command and Control Servers **December 2024**

I developed a Command and Control (C2) server to deepen my understanding of how botnets, like the Mirai Botnet (my case study), operate. The project focused on Linux systems and utilized Python's socketserver library to manage multiple connections. Bots compromised by an attacker maintain persistence by linking to the server and periodically checking a command file for instructions. This allows the botmaster to control thousands of machines by updating the file with new commands. Through this project, I gained insights into implants, TCP sockets, channel encryption, and leveraging platforms like GitHub and Discord for C2 operations.

Technical Blog Author **link:** https://medium.com/@karisallan237

I started writing on Medium, with my first article focusing on Google Dorking—how hackers use it to gather information for penetration testing. New articles have been dropped recently such as turning NMAP to a full vulnerability scanner.

SKILLS AND TECHNOLOGY

Technical skills: Data Analysis, AI(Prompt-Engineering, Langchain, RAG), Web Development, Network Design and Administration, Penetration Testing, Social Engineering, Reverse Engineering and Digital Forensics.
Frameworks: Data Analysis (Power Bi, MySQL, Excel), Flask, Security-Metaspoit, Maltego, Burp Suite, OWASP ZAP, NMAP Scripting Engine, Hashcat, and John the Ripper.
Programming: Python for Data Analysis, SQL, Shell Scripting (Python & Bash), and C/C++, x 86 Assembly, NIM, PowerShell, Batch, HTML, CSS and Java Script.
Soft skill: Time management, customer service, working under pressure, and group work.