ADEYINKA MOSOPE ADEJUMO

Networking & Security

+234 907 845 1018 | adejumoadeyinka35@gmail.com

linkedin.com/in/adeyinka-adejumo | github.com/Mosope-ade

SUMMARY

Computer Science & Engineering undergraduate focused on network security and defensive operations. Hands-on experience in incident response, packet analysis, and phishing simulation, with a habit of building practical security tooling in Python and Rust. Cisco and Google IT Support networking foundation.

PROJECTS

Argus — Agentic Incident Responder *Python, JavaScript*

LLM-driven SOC tool that turns a fired Splunk alert into a complete incident report in seconds — work that takes an analyst around two hours by hand.

- Runs autonomous investigations where the agent chooses each next step from the evidence rather than a fixed script, generating its own SPL queries at runtime to handle unknown alert types.
- Reconstructs the full attack chain as a chronological timeline, maps activity to MITRE ATT&CK across 40+ techniques, and correlates extracted IPs and domains against a bundled threat-intel dataset.
- Streams every agent decision live to the UI over WebSocket; triggered natively by Splunk saved-search webhooks; one-click PDF report export with browser notifications on critical findings.

netsniff — Packet Sniffer *Rust*

Command-line packet sniffer built in Rust on libpcap for raw-socket traffic capture.

- Parses the full stack from the Ethernet frame up — decoding IPv4/IPv6 (source, destination, protocol/next-header), TCP (ports, sequence number, window size, and SYN/ACK/FIN/RST flags), and UDP (ports, length), with ICMPv4/ICMPv6 detection.
- Captures on a selected interface with configurable packet counts (including continuous capture) and release-optimized builds for live use.

netwatch — Network Monitoring Dashboard *Python, Streamlit, Scapy*

Single-file, browser-based dashboard for real-time network monitoring and analysis, doubling as a pentest utility.

- Captures live traffic via Scapy in a rolling 10,000-packet window, tracks per-NIC upload/download bandwidth, and maps destination ports to services from live traffic.
- Discovers hosts on the subnet through a concurrent ICMP ping sweep with latency and reverse-DNS lookup.
- Exports captured packets to .pcap for Wireshark; configurable auto-refresh and per-interface (or all-interface) monitoring.

SECURITY & LAB EXPERIENCE

Targeted Phishing Simulation *Gophish*

- Designed and executed a controlled phishing campaign to measure user awareness and simulate real-world social engineering.
- Analyzed results to identify security gaps and recommend mitigations.

Systems Deployment & Hardening

- Installed and configured Windows and Linux systems on physical hardware, including drivers, security settings, and updates.

Virtualization & Lab Environment

- Built and maintained multiple virtual machines (including Linux) to run network simulations and support programming labs.

TECHNICAL SKILLS

Operating Systems: Kali Linux, Ubuntu, Windows 7 / 8.1 / 10, Android
Networking: TCP/IP, subnetting, routing, SSH, HTTP/HTTPS, DNS, DHCP
Programming: Python, Rust, Bash
Tools: Gophish, Scapy, libpcap, Wireshark, Splunk

CERTIFICATIONS

- Google IT Support Professional Certificate — Google / Coursera (In Progress)
- Introduction to Cybersecurity — Cisco Networking Academy

EDUCATION

Obafemi Awolowo University, Nigeria 2023 – 2028 (Expected)
B.Sc. Computer Science & Engineering

AltSchool Africa (Online) 2024 – 2025
Diploma in Cybersecurity