Bertrand Munihuzi Kalisa

216-972-0123 | bmkalisa@uark.edu | linkedin.com/in/bertrand-m-kalisa-992974152/ | github.com/bertrandka12

Education

University of Arkansas Fayetteville, AR
Master of Science in Computer Science *Expected May 2025*
Coursework: Machine Learning, Computer Vision, Cloud Computing and Security, Computer Security, Network Security, Privacy Enhancing Technologies, Advanced Database Systems.

Graduate Cybersecurity Certificate by University of Arkansas (expected by May 2025)

University of Arkansas Fayetteville, AR
Bachelor of Science in Computer Science *Jan. 2019 – Dec. 2021*
Coursework: Programming Foundations, Data Mining, Software Engineering, Mobile Programming.

Experience

Graduate Assistant, TA for Data Mining and Software Engineering Fayetteville, AR
University of Arkansas *Sept. 2023 – Present*

- Provide grading and feedback for over 50 students per semester, ensuring consistent assessment of assignments, sprints, exams and projects.
- Lead weekly office hours, helping students debug ML models and understand key concepts, improving course engagement.
- Guide student teams through semester-long software project using Agile/Scrum methodologies and practices, emphasizing sprint planning, task tracking (Trello), and collaborative coding (GitHub).

Computer IT Support Fayetteville, AR
University of Arkansas *Aug. 2019 – Dec. 2021*

- Provided hands-on technical support to 500+ students, troubleshooting software and hardware issues across multiple operating systems.
- Trained new lab operators, ensuring continuity of support for students navigating software challenges.
- Assisted in reporting technical issues through the university's ticketing system, improving efficiency in handling recurring software and hardware problems.

Projects

Packet Sniffing and Spoofing Lab | *Seed Labs| Python, Scapy, Wireshark*

- Developed packet sniffing program using Scapy (Python) and pcap (C) libraries to capture ICMP, TCP, and subnet-specific packets.
- Created spoofing tools to forge ICMP echo requests and implemented traceroute functionality using TTL manipulations.
- Combined sniffing and spoofing techniques to design a "sniff-and-then-spoof" program, which faked echo replies to ICMP packets for misdirecting ping responses.
- Used Wireshark to debug and validate packet capturing and spoofing, ensuring program reliability and accuracy.

SYN Flood Mitigation in P4 – Graduate Research Project | *Python, P4, Wireshark*

- Designed and implemented multiple SYN flood mitigation strategies in P4, including static thresholding, adaptive thresholding (WMA, EWMA), and blacklist/whitelist logic, on programmable switches.
- Developed per-IP stateful filtering using P4 registers and performed traffic analysis via Mininet and Wireshark to validate attack detection and packet drop behavior.
- Evaluated trade-offs in detection responsiveness, false positives, and system recovery time across thresholding methods, demonstrating improved mitigation precision with deterministic enforcement.
- Simulated attack traffic using hping3 and analyzed results via CLI registers and interface captures to assess defense efficacy under high-volume attack scenarios.

Languages, Technical Skills and Tools

Java, Python, SQL, Problem-solving, OOP, GitHub, Visual Studio, Eclipse, NumPy, Matplotlib, pandas for data visualization, Jupyter Notebooks, Google Colab, Scikit-Learn, Utilizing Agile methodologies and practices.