# Kisakye Kirabo

Cybersecurity Student · Rochester Institute of Technology
Laurel, MD ♦ 443-374-8053 ♦ kisakyekirabo.2024@gmail.com ♦ https://github.com/kkirabo/Portfolio

Objective: Cybersecurity student at RIT seeking a Summer 2026 cyber Internship/co-op. Interests in vulnerability assessment, network monitoring, and penetration testing, with hands-on experience in Linux, Windows Server, and virtual lab environments.

## Education

**Rochester Institute of Technology (RIT)** — **Rochester NY**
B.S. Cybersecurity, Minor in International Relations — Expected May 2028

**Eleanor Roosevelt High School** — **Greenbelt MD**
Science and Technology Program — Graduated May 2024

## Technical Skills

**Security & Networking:** Nmap, Wireshark, Metasploit, Kali Linux, DNS, SSL/TLS

**Systems:** Rocky Linux, Windows Server (AD DS, DNS), VMware Workstation

**Scripting:** Python, Java

**Services & Tools:** Apache, MailEnable, Rsyslog, Crond, Rsync, FTP, Samba, NFS, RAID, Cockpit, Git

## Cybersecurity Projects/Labs (pdf and code in github portfolio)

**Brick Wall Cyber Vulnerability Assessment**

- Assessed a simulated organization's network infrastructure and identified 4 security vulnerabilities in system configuration and access controls.
- Described likely threat actors, attack paths, and risk prioritization using impact/likelihood to recommend remediation steps.

**Linux Automation & Log Analysis Scripts (Python)**

- Developed Python scripts on Rocky Linux to parse log files, generate attacker reports, and flag suspicious login activity.
- Built command-line tools for ping testing, system reporting (network, FQDN, OS, Storage, CPU, memory), and symbolic link creation, reinforcing Linux administration and automation skills.

**Virtual Small-Business Network Lab (VMWare Workstation)**

- Built a lab network with AD/DNS server, web, mail, log server, storage, and two clients.
- Configured Apache web hosting, DNS records (A, MX, and PTR records), MailEnable (MTA/MDA), Rsyslog logging, RAID, firewall rules, and SSL /TLS.

**Penetration Testing Lab with msfvenom & Metasploit**

- Generated a malicious payload with msfvenom and used Metasploit to establish a remote session on a target VM in a controlled lab environment
- Demonstrated post-exploitation techniques such as credential capture (keylogger) and discussed ethical and legal considerations of penetration testing.

**SQL Injection on Vulnerable Web App (CTF-Style Lab)**

- Deployed a vulnerable web application and hit a “secret.txt” flag for a teammate, then exploited a command injection / SQL injection vulnerability via a ping feature.
- Used knowledge of PHP input handling and Linux command execution to exfiltrate the teammate’s hidden flag, strengthening understanding of web app vulnerabilities (OWASP-style).

## Leadership Experience

**Travel Soccer Team** - *Team Captain* — **Columbia MD**

- Led teammates during training and games, reinforced communication, discipline, and accountability.
- Supported teammates’ growth and maintained standards such as uniforms and punctuality.

**Destination Imagination -** *Team Member* — **Laurel MD**

- Collaborated on long-term engineering and creative challenges, including building simple machinery and stage props.
- Helped organize tasks and timelines to ensure the team met competition deadlines.

## Relevant Course Work

Introduction to Cybersecurity, Introduction to Routing and Switching, Systems Administration I, Software Development & Problem Solving I & II (Python, Java)