Youssef Sadek

- **551-241-8296**
- **youssefsadekyis@gmail.com**
- **Hazlet, NJ**
- **LinkedIn**
- **GitHub**
- **Portfolio**

PROFESSIONAL SUMMARY

Information Technology student focused on Cybersecurity with hands-on internship experience in security operations and vulnerability management. Experienced in enterprise vulnerability scanning, IDS/IPS monitoring, SIEM-based analysis, and automated security tooling. Strong foundation in SOC workflows, threat detection, scripting, and scalable security platform development. Actively pursuing CompTIA Security+ certification.

EDUCATION

Bachelor of Science in Information Technology May 2022 - Aug 2026

New Jersey Institute of Technology (NJIT) Newark, NJ

Relevant Coursework: Network Security, System Security, Operating Systems, Ethical Hacking, Linux, System Administration

TECHNICAL SKILLS

Languages: Python, Bash, JavaScript, C
Tools: Kali Linux, Security Onion, Nessus, OpenVAS, Nmap, Masscan, VMware, SQL, Prisma, Tailscale, PagerDuty
Concepts: Security Operations (SOC), Vulnerability Management, IDS/IPS, Incident Response Fundamentals, Network Security, Risk Prioritization (CVSS), Ethical Hacking

CERTIFICATIONS

CompTIA Security+ (SY0-701) – In Progress
Udemy: Complete Python Programming Certificate – Mar 2024

EXPERIENCE

Cybersecurity & Technical Operations Intern Jun 2025 - Sep 2025

David Zwirner New York, NY

- Supported security operations and vulnerability management for enterprise networks across multiple locations
- Engineered and maintained a global vulnerability monitoring system with backend APIs, frontend features, and automated scan workflows
- Deployed and managed distributed Raspberry Pi scanning agents using OpenVAS, Nmap, and Masscan for continuous network assessment
- Conducted recurring vulnerability scans, validated findings, and prioritized remediation using CVSS scoring
- Integrated PagerDuty alerting for high-severity vulnerabilities to support escalation and incident response workflows
- Collaborated through GitHub pull requests and code reviews, following Agile development practices
- Applied secure deployment, logging, and error-handling best practices to improve operational resilience

PROJECTS

Enterprise Global Network Scanning & Vulnerability Monitoring System Jun 2025 - Sep 2025

David Zwirner New York, NY

Technologies: NestJS, Node.js, TypeScript, Prisma, SQLite, Masscan, OpenVAS (GVM), Python, Cron, React, PagerDuty

- Engineered a full-stack vulnerability scanning platform enabling automated host discovery, assessment, and reporting
- Orchestrated a scanning pipeline combining Masscan and OpenVAS via Python–Node interoperability, scaling to 50,000+ hosts
- Improved scan throughput by approximately 30% while reducing failure rates through pipeline optimization
- Implemented cron-based scheduling to automate recurring scans, reducing manual effort by over 80%
- Integrated PagerDuty alerts with retry and backoff logic for reliable escalation of critical vulnerabilities
- Secured access using Passport-based authentication and delivered a lightweight React UI for scheduling and results review
- Developed automated setup scripts to deploy scanning agents and dependencies, reducing setup time by 2+ hours per deployment

Cybersecurity Virtual Lab Mar 2025 - May 2025

- Deployed a multi-VM lab environment using Kali Linux, Security Onion, and BasicPentesting1 via VMware
- Identified and exploited 36 vulnerabilities, including a ProFTPD backdoor, using Metasploit workflows
- Monitored IDS alerts in SGUIL and analyzed packet-level data to validate intrusion activity
- Correlated offensive activity with defensive detections to strengthen SOC investigation skills

Vulnerability Scanner Tool Jun 2024 - Aug 2024

- Developed a multithreaded Python-based vulnerability scanner detecting 20+ common web vulnerabilities
- Improved scan performance by approximately 20% using concurrency, randomized headers, and user-agent rotation