

# Pranav Mahesh

Little Rock, Arkansas | [pranavmiyengar@gmail.com](mailto:pranavmiyengar@gmail.com) | 501-551-2766 | [github.com/pmahesh29](https://github.com/pmahesh29) | [pmahe29.github.io](https://pmahe29.github.io) | [linkedin.com/in/pmahesh29](https://www.linkedin.com/in/pmahesh29)

## EDUCATION

### University of Arkansas, Fayetteville

Bachelor of Science in Computer Science | Cybersecurity Concentration

August 2021 - May 2025

GPA: 3.50 | Dean's List

## SKILLS

- **Programming & Databases:** Python, C++, PowerShell, MySQL
- **Security & Forensics Tools:** Wireshark, Zeek, Snort, CrowdStrike, ServiceNow, Metasploit, OWASP ZAP, Suricata
- **Operating Systems & Virtualization:** Kali Linux, Ubuntu, SEED Labs, VMware, pfSense
- **Cybersecurity Domains:** Incident Response (NIST), Threat Hunting, SIEM, IAM, Zero Trust

## WORK EXPERIENCE

### Application Support Intern | Arvest Bank

May 2025 - Present

- Led an intern team to develop a Splunk SIEM strategy for fraud detection, analyzing logs to identify attack patterns and coordinate incident response across teams, similar to vulnerability triage workflows.
- Managed SSL certificate lifecycle and compliance monitoring, ensuring timely patching and remediation of security vulnerabilities in production infrastructure.
- Developed automated Linux scripts for production systems, implementing security-focused configurations and monitoring solutions to detect anomalies and maintain system integrity.
- Created technical training materials on Python security practices for 100+ IT associates.

### Data Security Intern | Tyson Foods

May 2024 - August 2024

- Participated in vulnerability triage and incident response workflows alongside SOC analysts, analyzing security alerts to identify root causes and coordinate remediation strategies.
- Evaluated security configurations and risk exceptions in the CrowdStrike EDR platform, documenting security justifications and implementing controls to prevent data exfiltration.
- Audited enterprise security policy implementations using the CYERA platform, ensuring compliance with security standards and identifying configuration weaknesses.
- Developed Python automation for security data processing, reducing manual analysis time and improving the accuracy of threat assessments.

### Software Development Intern | Arvest Bank

May 2023 - December 2023

- Researched and presented Zero Trust security architecture recommendations to executive leadership, analyzing security controls and risk mitigation strategies.
- Developed web applications with security-first design principles, implementing authentication, authorization, and input validation controls to prevent common vulnerabilities.
- Built QA and issue-tracking tools for monitoring security vulnerabilities and tracking remediation efforts across development teams.

## PROJECTS

### Cyber Attack Simulation Home Lab

September 2025 - Present

- Built an isolated virtualized environment using VMware with Kali Linux, Metasploitable2, and pfSense for vulnerability research and detection engineering.
- Performed systematic vulnerability assessment, identifying and documenting 23+ vulnerable services across multiple attack surfaces.
- Developed custom Suricata IDS detection rules for attack pattern recognition, including SYN scans, backdoor connections, and exploit attempts.

### Cyber Pattern Labs

August 2024 - May 2025

- Led development on an open-source cybersecurity platform with a 6-person team, contributing 150+ commits via GitHub using collaborative workflows including pull requests, code reviews, and issue tracking.
- Built a React-based web application and integrated security lab infrastructure, implementing features for vulnerability training and hands-on security exercises.
- Developed lab scenarios covering OWASP Top 10 vulnerabilities, network security, cryptography, and system hardening using open-source tools (Metasploit, OWASP ZAP, Snort).