Mythreya Hardur Madhukeshwara

240-886-7232 | hm.mythreya@gmail.com | linkedin.com/in/hmmythreya | portfolio

Education

University of Maryland — College Park, MD
Masters of Engineering in Cybersecurity - Digital Forensics, Information Assurance — *Aug. 2024 - Present*

PES University — Bangalore, India
Bachelor's in Computer Science Engineering — *Dec. 2020 - May 2024*

Work Experience

Medlaunch Concepts LLC | Cybersecurity Specialist Intern — Jun. 2025 - Present
Remote (US)

- Conducted security testing on a web application, identifying 20+ bugs and vulnerabilities, including Broken Access Control, Certificate exposure, and Header misconfigurations, collaborating with developers to remediate issues.
- Led a team of 4 in conducting SAST, DAST, and code reviews to strengthen application security, resulting in a reduction of detected security bugs from 15 per 1,000 lines of code to 4 per 1,000 lines of code.
- Designed IAM groups and policies to implement role-based access control to AWS services across the organization, reducing misuse and unauthorized access by 65%, consolidating from overly permissive access to 70 policies.
- Configured and deployed AWS KMS, WAF, and AWS Shield to reduce security risks and strengthen cloud infrastructure, achieving compliance with ISO 27001, HITRUST and HIPAA.
- Performed penetration testing and vulnerability assessments using Nessus, delivering detailed reports on security gaps and providing actionable remediation steps improving the overall security posture.

University of Maryland Police Department | IT Analyst Intern — Jul. 2025 - Present
College Park, MD

- Resolved 50+ IT support tickets involving system and software troubleshooting, upgrades, and user support.
- Maintained uptime of Critical 911 servers and machines, ensuring 24/7 operational availability.
- Migrated 100+ systems from Windows 10 to Windows 11, performing hardware, BIOS and software upgrades.
- Managed IT hardware and software inventory for 300+ devices using an in-house inventory management system, ensuring accurate lifecycle tracking and reducing asset discrepancies by 30%.
- Used Microsoft Intune to bring 50+ laptops up to compliance, improving device security across the organization.
- Installed, configured, and set up MDC laptops in police vehicles, including cameras, recording software, VPN access, and automated triggers to ensure officer safety.
- Performed monthly vulnerability assessments using Nessus and InsightVM, documented findings, provided remediation recommendations, and coordinated with the IT Director to enhance the security of critical servers
- Delivered technical support and solutions to law enforcement officers, 911 operators, SOC analysts and Emergency Operation Center systems.

Projects

Home Lab and VPN setup | *Raspberry Pi 5, WireGuard, PIVPN*

- Successfully installed, configured, and secured Ubuntu Server 24.04.1 LTS on a Raspberry Pi 5
- Configured static IP addressing for the Raspberry Pi 5 and established port forwarding rules on the home router, enabling secure remote access for management, testing, and penetration testing activities.
- Installed and configured Damn Vulnerable Web Application (**DVWA**) and **Metasploitable 3** in the home lab environment, allowing for hands-on practice with **penetration testing** techniques and tools, such as **Metasploit, Nmap, Burp Suite, and Nessus**, within a safe and isolated environment.

Others

Certifications: **OSCP+**, **CompTIA Security+**, **HTB Pro - Dante**, **Qualys VMDR**, Cloud Computing 101

Tools and Technologies: Python (Proficient), C C++ Go (Beginner), Burpsuite, Zap, Nmap, Metasploit, Splunk, hashcat, netexec, gobuster, Wireshark, Bloodhound, Volatility, Autopsy, Git, Raspberry Pi, Docker.

Volunteer Work: Volunteered at the Physical Security Village during DEFCON 33, educating 100+ attendees with demonstrations of RFID cloning using a Flipper Zero to raise awareness of real-world vulnerabilities.

Community: Wrote and maintained a cybersecurity blog on projects and experiences, engaging with peers and building a following of 80+ with 2,000+ reads and 50+ likes through educational content.

Practical Labs and CTF Experience: 100+ Machines rooted in HTB and ProvingGrounds strengthening Enumeration, Web and Service Exploitation, Privilege Escalation, Lateral Movement, and AD exploitation. Participated in and won several CTFs, providing detailed writeups to challenges.