Mahesh Sanjay Udaykar

Pune, India | +91 9373289840 | maheshudaykar11@gmail.com
linkedin.com/in/mahesh-udaykar-75900425a | github.com/maheshudaykar

PROFESSIONAL SUMMARY

Electronics & Communication Engineering student (Graduating June 2026) with demonstrated hands-on experience in cybersecurity, vulnerability assessment, and secure systems development. Built production-oriented security tools including an AI-based phishing detection platform (research paper submitted), an AI-guided security audit automation framework, and a honeypot-based threat intelligence system. Skilled in VAPT, OWASP Top 10, network security, threat analysis, and Python-based security automation on Linux environments. Seeking entry-level roles as SOC Analyst, Security Analyst, or Junior Security Engineer.

TECHNICAL SKILLS

Cybersecurity: Vulnerability Assessment & Penetration Testing (VAPT), OWASP Top 10, Web Application Security, Threat Analysis, SOC Operations, Incident Response (Basic), OSINT, Threat Intelligence, Secure Testing Workflows, MITRE ATT&CK Framework

Security & Recon Tools: Burp Suite, Nmap, Wireshark, Metasploit, OWASP ZAP, Nuclei, Nikto, Semgrep, Bandit, Gitleaks, pip-audit

Networking & Protocols: TCP/IP, DNS, HTTP/HTTPS, Port Scanning, Packet Analysis, Traffic Monitoring, Client-Server Architecture, IDS/IPS Concepts

Programming & Scripting: Python (Security Automation, Networking, Tool Development), Bash Scripting, Embedded C (Basic)

Systems & Platforms: Linux (Kali Linux, Ubuntu), Raspberry Pi, WSL, Virtual Environments, CLI-based Systems

Architecture & Dev: REST APIs, WebSockets, Distributed Systems, Modular System Design, Flask, API Integration

AI & Applied Systems: Local LLM Integration (Ollama – Mistral, DeepSeek-Coder), AI Pipeline Orchestration, Basic ML (scikit-learn), Reinforcement Learning Concepts, Automation Workflows

Embedded & IoT: Microcontrollers, UART Communication, PWM Motor Control, Sensor Integration, Hardware-Software Interfacing

EXPERIENCE

Security Analyst Intern *Sep 2024 – Aug 2025*
Guru Branding Services, Pune

- Conducted end-to-end VAPT assessments on 4+ client web applications using Burp Suite, OWASP ZAP, and Nikto; identified 15+ security vulnerabilities including critical OWASP Top 10 flaws (SQL Injection, Broken Authentication, XSS, IDOR)
- Performed systematic network reconnaissance and service enumeration using Nmap; produced structured, client-facing vulnerability reports with proof-of-concept demonstration and prioritized remediation roadmaps
- Monitored application and system logs for threat indicators and anomalous activity; investigated suspicious patterns and supported incident response across 3 internal security events
- Assisted in system hardening by identifying and remediating misconfigurations across web server and application deployments, reducing exploitable attack surface
- Followed industry-standard VAPT methodology and secure testing workflows throughout all engagements; maintained documentation in line with professional reporting standards

Freelance Cybersecurity Analyst & Technical Consultant *2025 – Present*
Self-Employed (Clients: CodeServe Tech, GBS)

- Conducted independent security assessments for client web applications and systems applying structured VAPT methodology; delivered client-verified reports with actionable remediation and proof-of-concept evidence
- Identified vulnerabilities including input validation flaws, authentication misconfigurations, and exploitation vectors across multiple client environments
- Performed full-cycle reconnaissance, scanning, and analysis using Nmap, Burp Suite, and custom Python-based automation scripts

PROJECTS

Gojo – Hybrid AI Phishing Detection System *Ongoing | Research Paper Submitted*

- Developed production-grade phishing URL detection system combining heuristic rule-based analysis, machine learning, and reinforcement learning; achieved ~99% detection accuracy on ~50,000 URL dataset
- Implemented ensemble ML pipeline using lexical and character n-gram feature models; integrated Thompson Sampling-based contextual bandit for adaptive real-time learning and decision-making
- Engineered multi-layer detection architecture: feature extraction, content inspection, drift detection, and attack pattern recognition
- Built scalable system supporting real-time (~20ms latency) and bulk (10,000+ URLs/batch) analysis; exposed via REST API, CLI, and web interface – relevant to phishing and email threat detection workflows

Vulnara – AI-Guided Security Audit Automation Platform *Ongoing*

- Engineered local-first, extensible security audit platform for automated validation of web applications, APIs, and software packages; designed for repeatable and structured security assessment workflows
- Built multi-module testing engine integrating static analysis (Semgrep, Bandit), dynamic testing (OWASP ZAP, Nuclei), and dependency scanning (pip-audit, npm audit) in a unified pipeline
- Developed AI orchestration layer using local LLMs (Mistral, DeepSeek-Coder via Ollama) for automated test strategy generation, payload creation, and vulnerability reasoning
- Designed structured reporting engine producing exportable security assessment reports with actionable remediation insights

Honeypot Deployment & Threat Intelligence Analysis System *Completed*

- Engineered controlled honeypot environment simulating vulnerable systems to capture and analyze real-world attack traffic including brute-force attacks, reconnaissance scans, and exploitation payloads
- Performed behavioral analysis on attacker IPs, payloads, and access patterns; derived structured threat intelligence with centralized logging and analysis workflows
- Documented attack signatures and indicators of compromise (IOCs) for systematic threat intelligence reporting

Automated Network Reconnaissance & Vulnerability Mapping System *Completed*

- Developed Python-based automated reconnaissance framework leveraging Nmap for large-scale port discovery, service enumeration, and vulnerability surface mapping
- Designed structured reporting output supporting systematic analysis, risk prioritization, and further exploitation assessment workflows

THEO Rover – Hybrid Terrain Robotic System *Final Year Project | Ongoing*

- Architected dual-layer embedded control system: Raspberry Pi (orchestration, REST APIs, WebSocket communication) + microcontroller (deterministic real-time control) for multi-terrain navigation including stair traversal
- Developed full-stack control platform (Flask, WebSockets) with Cloudflare Tunnel for secure, globally accessible remote operation; engineered UART-based serial communication protocol for reliable command transmission
- Developing AI-assisted monitoring layer with OpenCV/YOLO for obstacle detection and terrain-aware adaptive navigation

Pi-hole Network-wide DNS Filtering & Traffic Intelligence System *Completed*

- Deployed Raspberry Pi-based DNS sinkhole for network-wide traffic filtering and monitoring; implemented DNS query analysis to identify suspicious domains and anomalous traffic patterns
- Enhanced network visibility through centralized logging; relevant to network monitoring and DNS-layer threat detection concepts applied in SOC environments

CERTIFICATIONS

- **Certified Network Security Practitioner (CNSP)** – The SecOps Group
- **Certified Security Expert Development Program (CSEDP)**
- *Currently pursuing:* Certified Ethical Hacker (CEH) – EC-Council

LEADERSHIP & ACTIVITIES

Technical Lead – Codement-24 Hackathon *2024*

- Led technical planning and execution of 24-hour intercollegiate hackathon with 50+ competing teams (~200 participants)

Technical Lead – Institution Innovation Council (IIC) *2023–2024*

- Spearheaded organization of technical workshops, innovation challenges, and startup-focused events at institutional level

Lead – Tech Talk Friday (Technical Podcast) *2024–2025*

- Managed end-to-end production of technical podcast covering cybersecurity, AI, and engineering topics; led content planning and speaker coordination

Additional: Actively engaged in CTF (Capture the Flag) challenges, cybersecurity labs, and hands-on security testing environments; continuously building practical exposure to real-world attack and defense scenarios.

EDUCATION

B.Tech in Electronics & Communication Engineering *2022 – 2026*
Nutan College of Engineering and Research, Pune
Relevant Coursework: Embedded Systems, Computer Networks, Operating Systems, Digital Electronics

HSC (Class XII) – 82.17% *2022*
Sahakar Vidya Mandir & Jr. College, Buldhana

SSC (Class X) – 83.80% *2020*
Sahakar Vidya Mandir, Buldhana