ANJAN KUNDURU

College Park, MD (open to relocation) · +1 240-791-6679 · anjanshiva9@gmail.com
linkedin.com/in/anjan-kunduru · github.com/anjanshiva2219

SUMMARY

Security engineer with an M.Eng in Cybersecurity (University of Maryland) spanning offensive and defensive security, and a habit of turning security work into code. Hands-on across full-scope penetration testing (web, API, network, cloud), secure code review, and threat detection. I write Python and Bash automation so that finding and fixing vulnerabilities scale instead of depending on one specialist by hand. Genuine AI/ML-security depth (97%-accuracy detection pipeline, ML/LLM attack-surface analysis) on top of real-world experience protecting the data of ~30,000 customers. I own problems end to end, quantify impact, and translate findings into clear, prioritized remediation.

SKILLS

- **Offensive Security:** Penetration Testing (Web/API/Network/Cloud), Red Team Operations, Exploit Development, Reverse Engineering, Privilege Escalation, Lateral Movement, Post-Exploitation, OSINT
- **Application & Cloud Security:** Secure Code Review, Threat Modeling, OWASP Top 10, SQLi/XSS/CSRF, Authentication & Authorization, API Security, AWS, IAM, Zero Trust, TLS/mTLS, SAST, DAST, DevSecOps
- **Security Automation & Tooling:** Python & Bash automation for vulnerability discovery, building security tooling, dependency scanning, CI/CD security integration, continuous/automated assessment
- **Detection, Response & Forensics:** SIEM & log analysis, SOC alert triage, incident response, threat hunting, IDS/IPS (Snort/Zeek), disk/memory forensics (Autopsy, Volatility), Wireshark
- **AI/ML Security:** AI/ML & LLM attack-surface analysis, adversarial ML, anomaly detection, ML-pipeline security, ML-driven security tooling
- **Networking:** HTTP, DNS, TCP/IP, packet analysis
- **Programming:** Python, Bash, C, Java, SQL, JavaScript
- **Frameworks:** OWASP, PTES, MITRE ATT&CK, NIST · ISO 27001 / SOC 2

EXPERIENCE

Security Engineer — Sports Excitement (Remote · Mar 2026 – present)

- Assess applications and APIs for OWASP Top 10, authentication/authorization, and insecure-cryptography flaws through testing and source-code review; partner with engineers to fix issues directly rather than handing off findings.
- Write Python and Bash automation for vulnerability discovery and repetitive assessment tasks, replacing manual review steps with repeatable, scalable checks.
- Integrate SAST, DAST, SIEM, and dependency-scanning tooling into a SOC 2 / ISO 27001-aligned workflow; analyze SIEM alerts and logs to triage and escalate threats.
- Support threat modeling and risk assessments for new features and third-party software.

Security Analyst — Tapojwalan Gas Agencies (Karimnagar, India · 2021 – 2023)

HP Gas (Hindustan Petroleum) authorized LPG distributor

- Owned information and IT security org-wide for a distributor serving ~30,000 customers, protecting endpoints, networks, and large volumes of sensitive customer PII through access controls and system hardening.
- Implemented preventive and detective controls; detected, investigated, and remediated multiple security incidents to restore secure operations.
- Served as primary security point of contact, advising staff on safe data handling and phishing awareness.

PROJECTS

Full-Scope Web, Network & Cloud Penetration Test (2024)

Burp Suite, Nmap, Metasploit, Impacket, Kali Linux

- Led a 3-person red team from reconnaissance and OSINT through post-exploitation across a simulated enterprise (Windows, Ubuntu, AWS cloud); exploited services via EternalBlue, dumped and cracked credentials, escalated privileges, moved laterally to domain admin, and exfiltrated data from a misconfigured S3 bucket.
- Delivered a professional report with CVSS-scored findings and a prioritized remediation roadmap.

Insider-Threat Detection Pipeline (2025)

Python, scikit-learn, TensorFlow

- Engineered an automated detection pipeline (Isolation Forest + LSTM Autoencoder) over user-activity logs, reaching 97% detection accuracy on the CERT Insider Threat dataset with no labeled attack data; proposed SHAP-based explainability and federated-learning privacy mitigations.

Digital Forensics & Incident Response Investigation (2025)

Wireshark, CyberChef, Volatility, VeraCrypt

- Reconstructed a full attack timeline end to end: captured live C2 HTTP traffic, decoded a Base64 encryption key, and used a file-signature mismatch to uncover a VeraCrypt container disguised as an .mp3, then decrypted it to recover the payload, scoring 30/30.

EDUCATION

University of Maryland, College Park — M.Eng in Cybersecurity (Jan 2024 – Dec 2025)

- Coursework: Penetration Testing, Network Security, Secure Operating Systems, Cloud Security, ML for Cybersecurity, Digital Forensics & Incident Response, Information Assurance

Sreenidhi Institute of Science and Technology — B.Tech, Electronics & Communication Engineering (2019 – 2023)

CERTIFICATIONS

Google Cybersecurity Professional Certificate · Cisco CCNA: Introduction to Networks · Cisco Python Certification · AWS Cloud Virtual Internship · AWS AI/ML Virtual Internship · Palo Alto Networks Cybersecurity Virtual Internship