AMAN KUMAR PANDA

Cybersecurity Practitioner | MCA Candidate | VAPT | Contact: +91-9937552371
Email: mnkmrpanda@gmail.com | Location: Vadodara, Gujarat LinkedIn: linkedin.com/in/amanpanda24
GitHub: https://github.com/AmanPanda24 | Portfolio: https://amanpanda24.github.io/portfolio/

PROFESSIONAL SUMMARY

Cybersecurity Practitioner and experienced in vulnerability assessment, penetration testing, and threat analysis across web, network, and system environments. Building multiple AI-powered security projects for real-time threat detection, OSINT automation, and misconfiguration scanning, showcasing both technical depth and practical problem-solving. Currently pursuing MCA in Cybersecurity & Forensic Science, eager to contribute to a security team focused on proactive defense and risk mitigation.

CORE COMPETENCIES

VAPT & Penetration Testing | Web Application Security | Network Security & Monitoring | OSINT & Threat Intelligence | Network Behavior Analysis | Security Tool Development | Digital Forensics | SIEM & Incident Response

TECHNICAL SKILLS

Languages:	Python, Bash, JavaScript, SQL, PHP
Penetration Testing:	Burp Suite, Metasploit, Nmap, OWASP ZAP, SQLmap, Gobuster, ExploitDB
Vuln. Assessment:	Nessus, OpenVAS, CVSS, CVE, Risk Prioritization
Web App Security:	OWASP Top 10, SQLi, XSS, CSRF, SSRF, XXE, Auth Bypass
Network Security:	Wireshark, TCP/IP, DNS, HTTP/HTTPS, Packet Analysis, VLANs, VPN
OSINT & Recon:	Maltego, theHarvester, Recon-ng, Shodan, WHOIS, Subdomain Enumeration, Passive Recon
Digital Forensics:	FTK Imager, Memory Forensics, Disk Imaging, Chain of Custody
OS & Platforms:	Kali Linux, Parrot OS, Ubuntu/Debian, Windows Server, TryHackMe, VulnHub, VirtualBox, VMware
Frameworks:	MITRE ATT&CK, OWASP Testing Guide, NIST CSF, ISO 27001, CVSS, SDLC, Threat Modeling

PROFESSIONAL EXPERIENCE

Cybersecurity Intern & Professional Trainee

Jul 2024 – Dec 2024

Hacker School (Cartel Software) Jayanagar, Bangalore

- Completed 200+ hours of intensive training in ethical hacking, VAPT, threat analysis, and incident response across web, network, and system domains.
- Performed manual and automated penetration tests using Burp Suite Pro and OWASP ZAP; identified SQLi, XSS, CSRF, SSRF, and auth bypass vulnerabilities with CVSS v3 scoring.
- Simulated real-world attacks across 7 threat categories via Metasploit; conducted network recon with Nmap/Nessus; performed traffic analysis via Wireshark for IoC detection.

Operations & HR Intern

Jun 2024 – Sep 2024

IKKASA, Remote

- Managed end-to-end recruitment and onboarding for 15+ new hires; developed standardized HR documentation templates reducing administrative overhead by ~30%.
- Maintained structured employee records and reporting summaries, demonstrating data organization and process discipline transferable to security operations.

PROJECTS

Aegis-AI — Intelligent Network Behavior Analysis & Detection System

https://github.com/AmanPanda24/Aegis-AI

(Python · scapy · Zeek/Suricata · Isolation Forest · XGBoost · LSTM · FastAPI · Kafka · WebSocket · Grafana)

Architected a 4-layer AI-powered NBA prototype (Packet Capture ▪ DPI ▪ ML Inference ▪ Dashboard) across a 3-VM isolated lab; extracted 13 features (Shannon entropy, inter-arrival time, TCP flags, payload entropy). Hybrid ML engine: Isolation Forest for zero-day detection, XGBoost (85%+ accuracy, CIC-IDS2017) for 7 attack classes, LSTM for low-and-slow APT detection; real-time threat scoring (0–100) with 4-tier risk classification.

Impact: End-to-end detection pipeline with sub-second ML inference across 7 attack categories.

PhantomEye. | AI-Powered OSINT Intelligence Framework

https://github.com/AmanPanda24/phantomeye

(Python · AsyncIO · REST APIs · DNS · Web Scraping · OpenAI LLM)

Modular async OSINT framework with plugin architecture for domain recon, social media enumeration, and threat correlation; async HTTP client with rate limiting, retry logic, proxy support, and JSON/CSV/HTML output. Integrated OpenAI LLM for automated pattern recognition and natural-language executive security summary generation.

Impact: Automated OSINT correlation and AI-generated summaries cut manual triage time significantly.

SecProbe | AI-Assisted Web Security Misconfiguration Scanner

https://github.com/AmanPanda24/SecProbe

(Python · Flask · REST API · Google Gemini · Groq LLaMA)

Automated scanner detecting missing HTTP security headers, SSL misconfigurations, and exposed ports with CVSS-style risk scoring; Flask REST API with JSON/HTML report export. Integrated Google Gemini and Groq LLaMA for AI-driven vulnerability explanation, impact assessment, and remediation guidance.

Impact: Bridges scanning and remediation with instant AI-generated fix recommendations.

EDUCATION

MCA — Cybersecurity & Forensic Science

Aug 2025 – Jul 2027 (Expected)

Parul University, Vadodara

BCA — 7.7 CGPA

Aug 2022 – Jul 2025

Sambalpur University, Odisha

CERTIFICATIONS & TRAINING

- **Certified Ethical Hacker (CEH) v12** - EC-Council (Completed 2024)
- **Certified Cybersecurity Professional** - ICTRD
- **Cybersecurity Professional Training** - Hacker School