Anant Kumar Pandey

Portfolio: anantsec.netlify.app
Email:anant.pandey017@gmail.com
GitHub: github.com/sh4dowkey
Address :Bhubaneswar (OD)
LinkedIn: linkedin.com/anant-ku-pandey

EDUCATION

- Trident Academy of Technology: Bhubaneswar (OD) ,India
  - Degree: Bachelors Of Technology (B. Tech) - Computer Science 2022 - 2026
- St. Mary's Higher Secondary School: Jharsuguda (OD) ,India
  - 12th - Grade – 90% 2021 – 2022

SKILL SUMMARY

- **Programming** :Python ,Go ,Bash, Java, C , C++, SQL, JavaScript, HTML/CSS.
- **Soft Skills** : Report Writing, Technical Documentation, Communication, Problem Solving, Analytical Thinking, Team Collaboration.
- **Skills** : Vulnerability Assessment & Penetration Testing (VAPT), Web Application Security, Network Security, Active Directory Security, Credential Harvesting, Lateral Movement, Kerberoasting, Privilege Escalation, Reconnaissance & OSINT, Recursive Crawling, Parameter Harvesting, OWASP Top 10 Testing, Incident Response, SIEM Log Analysis, Threat Detection, Risk Assessment, Security Automation, CLI Tool Development, Adversary Simulation, MITRE ATT&CK .
- **Tools :** Burp Suite, Nmap, Wireshark, Metasploit, Nessus / OpenVAS, BloodHound, Impacket, Responder, Netcat, OpenSSL, Shodan, theHarvester, DNSdumpster, Gobuster, Git, GitHub, Linux, GDB (Pwndbg).

CERTIFICATES

C|CT : Certified Cybersecurity Technician — EC-Council (Credential ID : ECC9285371640)

GCPC : Google Cybersecurity Professional Certificate — Google (Credential ID : 69LDJC7T49HZ)

API-Sec : OWASP API Security Top 10 and Beyond — APISec University

Other Certs : DataCom Cybersecurity Virtual Experience , Deloitte Cybersecurity Virtual Internship , Mastercard Cybersecurity Virtual Experience , Tata Cybersecurity Virtual Experience.

EXPERIENCE

- Teachnook — Cyber Security Intern . Remote - India
  (Cyber Security Intern) February 2025 – April 2025
  - **Responsibilities** : Reconnaissance, vulnerability assessment, and exploitation validation across web and network environments; automating recursive crawling and parameter harvesting using a custom Python CLI tool to support OSINT and attack surface mapping. Simulating security alerts and performing basic SOC-style triage workflows; documenting findings, remediation steps, and security hardening recommendations for web and network assets.

- AICTE-Edunet Foundation, IBM — Cyber Security Intern . Remote - India
  (Cyber Security Intern) January 2025 – February 2025
  - **Responsibilities:** Reconnaissance, vulnerability assessment, and exploitation validation across web and network environments; automating recursive crawling and parameter harvesting using a custom Python CLI tool to support OSINT and attack surface mapping. Simulating security alerts and performing basic SOC-style triage workflows; documenting findings, remediation steps, and security hardening recommendations for web and network assets.

PROJECTS / OPEN- SOURCE CONTRIBUTIONS

- Pwndbg **:- GDB Enhancement Tool (Open-Source Contribution)** : Refactored the symbol module with subcommands to improve CLI usability and modularity; aligned CLI behaviour with modern debugging workflows and open-source standards. Contributed production-ready code , collaborated with maintainers, and merged changes after positive code review . Technologies: Python, GDB, Git.
- CrawlX :- **Concurrent Web Crawler (Go)** : Built a performance-focused CLI crawler using goroutines and worker patterns; implemented recursive crawling, URL resolution, and concurrency controls for scalable reconnaissance. Added cross-platform install scripts and structured documentation; designed recon automation for OSINT workflows.
- CLI Web Crawler :- **Reconnaissance Tool (Python)** : Developed a feature-rich crawler for OSINT and vulnerability reconnaissance with depth-limited crawling, endpoint extraction, robots.txt handling, and export options (TXT/JSON/CSV). Integrated progress tracking and optional GUI module; documented full usage and modular repo structure.
- Secure Suite :- **Integrated Security Toolkit** : Built a unified toolkit combining reconnaissance adapters, encryption helpers, and a steganography module (StegoHide) implementing AES/RSA hybrid encryption with pixel-level encoding and password-protected extraction. Delivered CLI and lightweight GUI interfaces; demonstrates applied cryptography and tooling integration.