ANANT KUMAR PANDEY

anant.pandey017@gmail.com
Jharsuguda, IN 768201
+91-9337056057

LinkedIn: www.linkedin.com/in/anant-ku-pandey |
WWW: https://sh4dowkey.github.io

SKILLS

- **Cybersecurity**: red-team techniques, penetration testing, vulnerability assessment, credential harvesting, lateral movement, Kerberoasting, OSINT, exploit research.
- **Web & Recon:** recursive crawling, parameter harvesting, robots.txt handling, automated reconnaissance workflows.
- **Tools & Frameworks:** Burp Suite, Nmap, Wireshark, Metasploit, Nessus / OpenVAS, OpenSSL, BloodHound, Shodan, theHarvester, DNSdumpster, Gobuster, Netcat, Impacket, Responder.
- **Programming & Scripting:** Python (Advanced), Go (Intermediate), Bash, Java, C; Familiar with C++, SQL, JavaScript, HTML/CSS.
- **Other:** Git/GitHub, CLI tooling, OWASP Top 10, GitHub Actions, Linux fundamentals, Cyber Range labs (TryHackMe, Hack The Box).
- **Additional:** Vulnerability assessment, social engineering awareness, report writing, basic SIEM/ELK familiarity, incident response documentation.

SUMMARY

Proactive cybersecurity enthusiast with practical experience in vulnerability assessment, red-team techniques, and security automation. Skilled at building tools in Python and Go, designing/maintaining an Active Directory attack-defense lab, and performing reconnaissance and SIEM log analysis. Comfortable across offensive and defensive workflows; actively pursuing EC-Council C|CT certification.

WEBSITES, PORTFOLIOS, PROFILES

- sh4dowkey.github.io
- github.com/sh4shadowkey
- linkedin.com/in/anant-ku-pandey

WORK HISTORY

CYBERSECURITY CERTIFICATE & CAPSTONE

Teachnook | Remote — FEB 2025 - MAR 2025

- Completed instructor-led lectures and hands-on lab modules; delivered a capstone focused on vulnerability assessment and incident response workflows.
- Performed network discovery and vulnerability scanning (Nmap, Nessus/OpenVAS), prioritized findings by risk, and produced remediation guidance.
- Built and used a CLI web crawler for reconnaissance and parameter harvesting; practiced OWASP Top-10 exploitation in custom lab setups.
- Simulated alerts and performed basic triage workflows in a lab SIEM environment.

CYBERSECURITY CERTIFICATE & CAPSTONE

AICTE-Edunet Foundation, IBM | Remote — JAN 2025 - FEB 2025

- Completed IBM-aligned curriculum with practical labs on web app testing, network security, and AD attack/Défense basics.
- Built a lab-based detection scenario for lateral movement (using Responder & BloodHound) and created detection notes and suggested firewall/ACL changes.
- Produced a final project report demonstrating findings, remediation steps, and lessons learned.

EDUCATION

EXPECTED IN JUN 2026

B. Tech

Computer Science | Trident Academy of Technology | Bhubaneswar
GPA: 8.2

APR 2022

12th

St. Mary's Higher Secondary School | Jharsuguda, India

Final Grade:90%

APR 2020

10th

St. Mary's Higher Secondary School | Jharsuguda, India

Final Grade:92%

OPEN-SOURCE CONTRIBUTIONS

- Open-Source Contributor – Pwndbg (GDB Enhancement Tool)
- Refactored the symbol module with subcommands to enhance CLI usability and modularity.
- Aligned CLI behaviour with modern standards for advanced debugging flows.
- Followed open-source best practices: Ruff formatting, testing, and documentation.
- Collaborated with maintainers; merged post positive code review.
- Technologies: Python, GDB, Git, argparse, OSS workflows
- GitHub: https://github.com/pwndbg/pwndbg

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- EC-Council C|CT – In Progress
- Other Certifications: DataCom Cybersecurity Virtual Experience, Deloitte Cybersecurity Virtual Internship, Mastercard Cybersecurity Virtual Experience, Tata Cybersecurity Virtual Experience, OWASP API Security Top 10 and Beyond by APISec University

PROJECTS & LAB EXPERIENCE

CrawlX — Go (Concurrent Web Crawler) - [View on GitHub]

- Performance-focused CLI crawler implemented with goroutines and worker patterns.
- Implements recursive crawling, URL resolution, concurrency controls, and cross-platform install scripts (setup.sh, setup.ps1).
- Repo highlights: cmd/ sources, go.mod, install scripts, README with usage and roadmap (robots.txt support, JSON/CSV exports).
  Impact: Demonstrates Go concurrency, CLI design, and engineering for scalable reconnaissance.

CLI-Web-Crawler — Python (Reconnaissance Crawler) - [View on GitHub]

- Feature-rich Python crawler for OSINT & vulnerability reconnaissance: depth-limited recursive crawl, parameter/endpoint extraction, robots.txt handling, custom user agents, export options (TXT/JSON/CSV), progress tracking, and optional GUI module.
- Repo highlights: cli.py, crawler/ sources, Gui/, requirements.txt, detailed usage README.
  Impact: Shows security tooling, Python engineering, and practical recon workflows.

Active Directory Attack–Defense Lab — Multi-VM AD Lab - [View on GitHub]

- Full lab setup and documentation for enterprise AD attack/defense practice: DC and client configuration, attack playbooks, detection heuristics, and automation scripts.
- Repo structure includes attacks/, bloodhound/, detection/, scripts/, and step-by-step setup documentation.
  Impact: Validates hands-on experience with real AD attack techniques and blue-team detection notes.

SECURE SUITE — integrated security toolkit (includes StegoHide steganography module) – [View on GitHub]

- Integrated a collection of security utilities (image steganography module, recon crawler adapters, encryption helpers) into a single toolkit for secure demonstrations and automation.
- StegoHide module: AES/RSA hybrid encryption + pixel-level encoding/decoding, password-protected extraction, CLI and lightweight GUI interfaces, automated test vectors and demo images.
- Implemented integration hooks with crawler tools (recon adapters) and provided documentation for module testing and demo workflows.