ANANT KUMAR PANDEY

+91-9337056057 | anant.pandey017@gmail.com

Portfolio: sh4dowkey.github.io | GitHub: github.com/sh4dowkey

LinkedIn: linkedin.com/in/anant-ku-pandey

SUMMARY

Aspiring Cybersecurity Analyst Intern with hands-on experience in penetration testing, vulnerability assessment, red teaming, and security automation. Developed tools in Python and Go for OSINT, reconnaissance, and secure data hiding. Built and maintained an enterprise-grade Active Directory attack-defense lab. Adept at using tools like Burp Suite, Wireshark, Nessus, Metasploit, and BloodHound. Familiar with SIEM tools and risk analysis workflows. Strong problem-solving, analytical thinking, and effective communication skills.

EDUCATION

- B.Tech in Computer Science – Trident Academy of Technology, Bhubaneswar | 2022 – Present | CGPA: 8.2
- 12th – St. Mary's Higher Secondary School, Jharsuguda | 2022 | 90%
- 10th – St. Mary's Higher Secondary School, Jharsuguda | 2020 | 92.4%

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

SKILLS

- Cybersecurity: Offensive Security, Web Application Pentesting, Red Teaming, Threat Intelligence, Active Directory Attacks & Defense, Secure Data Hiding, Information Gathering, Exploit Development, OSINT
- Tools & Frameworks: Burp Suite, Nmap, Wireshark, Metasploit, Nessus, 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 Tools, OWASP Top 10, GitHub Actions, Linux Fundamentals, Cyber Range Labs (THM, HTB)

PROJECTS

- CLI Web Crawler – Python, BeautifulSoup, Requests, urllib, argparse
  - Developed a feature-rich terminal-based web crawler to aid in vulnerability reconnaissance and parameter harvesting.

- Supports depth-limited recursive crawling, CLI argument parsing, parameter extraction, colored output, and domain filtering.
- Logs discovered URLs, endpoints, and parameters for potential fuzzing or security testing.
- GitHub Repo: https://github.com/sh4dowkey/CLI-Web-Crawler

- StegoHide (Steganography Tool) – Python, OpenCV, Tkinter, PIL
  - Built a secure image steganography GUI that hides text inside images with pixel-level encoding.
  - Enabled AES/RSA-based encryption with password authentication before extraction.
  - Integrated image processing and drag-drop GUI for ease of use.
  - GitHub Repo: https://github.com/sh4dowkey/STEGANOGRAPHY
- Active Directory Attack & Defense Lab – Windows Server, Kali Linux, BloodHound
  - Deployed a virtual enterprise AD lab simulating real-world infrastructure to practice red and blue team exercises.
  - Performed enumeration, privilege escalation, and lateral movement using tools like BloodHound, CrackMapExec, Mimikatz, and Responder.

TRAINING PROJECTS

- Cybersecurity Capstone – AICTE-Edunet Foundation | Remote | Jan–Feb 2025
  - Built a full-featured steganography tool in Python using AES/RSA encryption methods.
  - Conducted network scans and cryptographic simulations using OpenSSL, Wireshark, and Nmap.
  - Practiced threat modeling and data confidentiality use cases in simulated environments.
- Cybersecurity Capstone – Teachnook | Remote | Feb–Mar 2025
  - Engineered a CLI-based web crawler from scratch; implemented recursive crawling, parameter extraction, and OSINT techniques.
  - Practiced exploiting OWASP Top 10 vulnerabilities in custom lab setups and CTF scenarios.
  - Hands-on experience with Burp Suite, Metasploit, DVWA, and multiple attack vectors.

OPEN-SOURCE CONTRIBUTIONS

- Open Source Contributor – Pwndbg (GDB Enhancement Tool)
  - Refactored the cymbol module with subcommands to enhance CLI usability and modularity.
  - Aligned CLI behavior 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