ANANT KUMAR PANDEY

+91-9337056057 | pandeyanant733@gmail.com | Portfolio: sh4dowkey.github.io | GitHub: github.com/sh4dowkey| LinkedIn: linkedin.com/in/anant-ku-pandey

SUMMARY

Aspiring cybersecurity professional with a strong focus on offensive security, penetration testing, and red teaming. Hands-on experience with Active Directory attack labs, web vulnerability scanning, and Python- and Go-based security automation. Skilled in using industry tools like Burp Suite, Nmap, and BloodHound. Eager to contribute to real-world VAPT or red team projects while continuously advancing technical expertise.

EDUCATION

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

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- EC-Council C|CT – In Progress

SKILLS

- Cybersecurity: Offensive Security, Web Pentesting, Threat Analysis, Risk Assessment, Reconnaissance, Secure Data Hiding, Active Directory Attacks & Defenses
- Tools & Technologies: Wireshark, Nmap, Burp Suite, Metasploit, Nessus, OpenSSL, Shodan, BloodHound, theHarvester, DNSdumpster
- Programming: Python (Proficient), Java, C, Go; Familiar with C++, SQL, JavaScript

PROJECTS

- StegoHide – Python, OpenCV, Tkinter, PIL
  Developed a GUI tool for encrypting and hiding text in images using pixel encoding and password protection.
- CLI Web Crawler – Python, Requests, BeautifulSoup, urllib
  Built a terminal tool for link discovery and parameter extraction to aid in web vulnerability scanning.
- AD Attack-Defense Lab – Windows Server, Kali, BloodHound
  Simulated an enterprise Active Directory environment to practice red team tactics and implement layered blue team defenses.

TRAINING PROJECTS

- Cybersecurity Capstone – AICTE-Edunet Foundation | Remote | Jan–Feb 2025 ‣ Built a Pythonbased steganography tool using AES/RSA.
  - ‣ Conducted network scanning and cryptographic simulations using Nmap, OpenSSL, and Wireshark.
- Cybersecurity Capstone – Teachnook | Remote | Feb–Mar 2025
  - ‣ Created a CLI web crawler and practiced OWASP Top 10 vulnerabilities in lab setups.
  - ‣ Used tools such as Burp Suite, Nmap, and Metasploit for hands-on exploitation and CTF-style labs.