Tanish Choudhary

Jodhpur, Rajasthan • +91 9358413124

EDUCATION

Delhi Public School, Jodhpur   *2021 – 2022*
Completed 10+2 with PCM & CS   *Jodhpur, Rajasthan*

Dehradun Institute of Technology   *August 2022 – present*
Bachelor of Technology in Computer Science Engineering   Dehradun, Uttarakhand

PROFILE LINKS

Email : tanishch21@gmail.com
TryHackMe : tryhackme.com/p/TANISHRJ
Github :   github.com/TanishRj/
Linked-In : linkedin.com/in/tanish-choudhary/

EXPERIENCE

Cyber Security Intern
Amroha Police Cyber Security Internship Program   *June 2025*
- Gained real-world exposure to cybercrime investigations.
- Received hands-on training in digital forensics and evidence analysis.
- Explored new cybersecurity topics and investigative tools.

CERTIFICATIONS & ACHIEVEMENTS

- **TryHackMe** : Top 3%, Rank **46,758**, **23 badges**, **120+ rooms solved** (2024 Moniker Link CVE, FlareVM)
- **THM Certifications** : Jr. Penetration Tester, Cybersecurity 101, Pre-Security, Web Fundamentals, Intro to Cybersecurity
- **EC-Council –** Introduction to Dark Web and Anonymity
- **AIG Forage :** Decrypt Ransomware, Phishing Campaign, Cyber Security Management, APT Breach Analysis
- **Port-Swigger –** 50+ Web Security Lab Solved
- **Competition :** 2nd Place in ATL Marathon (India-Wide) – "Covid Testrone" Project

SKILLS

- **Programming & Scripting** : Java, Python, C, Bash, Go-lang (knowledge), MySQL, JavaScript, HTML, CSS
- **Offensive Security Tools** : Metasploit, Nmap, Hydra, SQLmap, Burp Suite, Nikto, Dirbuster, Gobuster, John the Ripper, Hashcat, Mimikatz, Kerbrute, LaZagne, WinPEAS, LinPEAS
- **Red Teaming & Post Exploitation** : Impacket, BloodHound, Responder, Chisel, PsExec, Socat, Active Directory Security, Pivoting, Post-Exploitation and pivoting Techniques.
- **OSINT Tools** : Shodan, Maltego, Google Dorking, AssetFinder, Amass, Sublist3r, Httprobe, Knock
- **Wirelesss & Network Security** : Wireshark, Aircrack-ng, Masscan, Hping3, WPScanner
- **Malware Analysis & Reverse Engineering (knowledge)** : Process Monitor, PE Studio and Process Hacker

PROJECTS

- **Port Scanner**
  - Developing a custom **network scanning tool** to identify **open ports, services, and vulnerabilities**.
  - Implements **multi-threading** for fast scanning and integrates **Nmap-like functionality**.
  - Aims to automate reconnaissance and vulnerability assessment for **penetration testing engagements**.

- **Threaded SSH Bruteforcer**
  - Developed a multi-threaded SSH Brute-force tool for efficient login attempts.
  - Supports custom wordlists and parallel credential testing.
  - Useful for red teaming and assessing SSH password strength.