Mohammed Tauseef Ahmed

Penetration Tester

✉ tsfahmd01@gmail.com ☎+91 90529 72697 in linkedin.com/in/tsfahmd01
★Portfolio: tsfahmd001.github.io/portfolio/
github.com/tsfahmd001 medium.com/@tsfahmd01 ⌂Hyderabad, India

Profile Summary

An entry-level offensive security professional with hands-on experience in penetration testing and vulnerability assessment. Certified eJPT, demonstrating applied knowledge of reconnaissance, exploitation and post-exploitation. Built a pentesting lab (Kali, Metasploitable, OWASP Juice Shop), practiced real-world attack scenarios & published pentest reports. Active CTF participant with proven problem-solving skills under time constraints. Seeking a Junior Penetration Tester role with opportunities to grow into advanced offensive security and red team engagements.

Technical Skills

- **Security Tools:** Nmap, Nessus, Metasploit, Hydra, GoBuster, Burp Suite, Wireshark, John-the-Ripper
- **Languages:** C++, Python, Bash
- **Platforms:** Linux (Kali & Parrot), Windows
- **Frameworks:** OWASP Top 10, MITRE ATT&CK
- **Reporting:** Pentest reports, findings matrix, risk impact analysis, remediation guidance.
- **Web/Database:** HTML/JS, SQL

Certifications

- eJPT (INE - eLearnSecurity Junior Penetration Tester) Oct 2025
- Google Cybersecurity Certificate (V2) Mar 2025

Education

B.Tech in CSE (AI & ML)
CMR College of Engineering and Technology 2021–2025

Experience

Offensive Security and Pentesting Simulations (Self-Directed) Jan 2025–Present

- Built a local pen-testing lab using Kali, Metasploitable & OWASP Juice Shop, published redacted reports on GitHub.
- Completed 100+ TryHackMe rooms, including Junior Penetration Tester and Web Fundamentals learning paths, covering reconnaissance, vulnerability assessment, exploitation and reporting.
- Earned eJPT (eLearnSecurity Junior Penetration Tester) certification, demonstrating hands-on proficiency in real-world pentest workflows.
- Active Capture the Flag (CTF) competitor; solved challenges across web exploitation, binary analysis, cryptography, and forensics under time constraints.

Projects

LoMar: A Local Defense Against Poisoning Attacks on Federated Learning
Presented at ICRETM'25

- Demonstrated federated learning client compromise in a safe lab environment.
- Designed a defense using KDE (Kernel Density Estimation) on CNN feature embeddings for anomaly detection.
- Enhanced robustness against label-flipping and stealth poisoning attacks, improved accuracy from 90.1% to 97.0%.

TryHackMe Labs & Capture The Flag (CTF) Challenges

- Completed 100+ TryHackMe rooms; mastering reconnaissance, enumeration, exploitation and post-exploitation.
- Focused on Jr Penetration Tester and Web Fundamentals learning paths to align with real-world techniques.
- Ranked among top 4% of TryHackMe users.
- Regularly participate in CTF competitions, covering web, privilege escalation, binary and cryptography.

Penetration Test Simulations

- Conducted simulated blackbox pentests; reconnaissance, enumeration, exploitation & privilege escalation.
- Documented multiple misconfigurations leading to full system compromise.
- Authored professional redacted reports including executive summary, findings matrix and remediation roadmap.