HEM Nikesh GABHAWALA

Vadodara, Gujarat, India
Email: hemgabhawala@icloud.com | Phone: +91 95125 37083
LinkedIn: https://www.linkedin.com/in/hem-nikesh-gabhawala-99a5482a9/ | GitHub: https://github.com/securitywithhem | TryHackMe: https://tryhackme.com/p/SecurityWithHem

OBJECTIVE

Motivated Cybersecurity Enthusiast with hands-on experience in ethical hacking, vulnerability assessment, and penetration testing. Certified by Google and active on TryHackMe, I aim to apply my attacker mindset and technical skills in a professional environment to help secure applications and networks while gaining practical industry experience.

KEY SKILLS

Technical Tools: Nmap, Burp Suite, Wireshark, Metasploit, Nikto, OWASP ZAP, Hydra
Programming & Scripting: Python, Bash, SQL, Java (basic)
Security Concepts: Vulnerability Assessment (VAPT), Threat Modeling, Incident Response, Network Security, Linux Hardening
Operating Systems: Kali Linux, Ubuntu, Windows Server
Soft Skills: Analytical Thinking, Team Collaboration, Documentation, Problem Solving

PROJECTS

Network Reconnaissance Tool (Python)
- Built an automated tool for subdomain enumeration and port scanning integrating Nmap and custom socket checks.
- Improved discovery speed with multi-threading and result filtering for actionable findings.

Personal TryHackMe Labs

- Completed 50+ rooms covering web exploitation, privilege escalation, network attacks, and blue team defensive tasks.

EDUCATION

Bachelor of Technology (B.Tech) – Computer Science Engineering
Navrachana University, Vadodara — 2022–2026 (Ongoing)
Relevant Coursework: Network Security, Operating Systems, Database Management Systems, Computer Networks

CERTIFICATIONS

- Google Certified Cybersecurity Professional
- TryHackMe: Jr. Penetration Tester, Web Fundamentals,
- Introduction to Ethical Hacking – Coursera / EC-Council (self-study)

ACHIEVEMENTS

- Completed 170+ TryHackMe rooms across offensive and defensive tracks.
- Organized a cybersecurity awareness workshop at Navrachana University.
- Actively participating in bug bounty practice and CTF challenges.

EXPERIENCE

Open to Internship Opportunities — Cybersecurity / Penetration Testing / SOC Roles
- Eager to apply skills in web app testing, network scanning, and automation to contribute to real engagements.
- Comfortable producing technical reports and communicating findings to technical and non-technical stakeholders.

INTERESTS

Bug Bounty Hunting | Ethical Hacking | Red Teaming | Security Startups | Automation & Scripting in Security