# Manthan Bhatt

+91 7046038802 | bhattmanthan8@gmail.com | Vadodara, Gujarat, India | LinkedIn | GitHub | Portfolio

## SUMMARY

Second-year B.Tech Computer Science student with hands-on experience in penetration testing, web application security, Linux post-exploitation, and network analysis. Built an original red team framework (L.E.A.P.) in Bash, competed in global CTF competitions, and completed the TryHackMe Jr Penetration Tester path. Holds certifications in ethical hacking, networking, and cybersecurity. Seeking a summer 2026 internship in penetration testing, vulnerability research, or security engineering.

## SKILLS

**Programming Languages** Python, Bash, C, C++, Java
**Security Tools** Nmap, Burp Suite, Metasploit, Wireshark, Gobuster, Netcat
**Dev and Version Control** Git, GitHub, Linux Command Line
**Security Domains** Penetration Testing, Web Application Security, Post-Exploitation, Privilege Escalation, Network Enumeration, Packet Analysis, Container Security, Vulnerability Assessment
**Web Vulnerabilities** SQL Injection, Cross-Site Scripting (XSS), IDOR

## EXPERIENCE

**Technical Team Member** Sep '25 — Present
GDG on Campus, Nirma University Ahmedabad, Gujarat, India

- Contributed to technical workshops, developer events, and knowledge-sharing sessions under Google Developer Groups on Campus at Nirma University.
- Secured 3 external sponsorships through targeted partnership proposals before event cancellation — full outreach, negotiation, and documentation completed professionally.

**Vulnerability Researcher** Jan '25
BugCrowd Platform India (Remote)

- Identified and documented a security vulnerability as part of a structured bug bounty competition hosted on Bugcrowd.
- Authored a formal vulnerability report covering reproduction steps, risk assessment, and remediation recommendations simulating a real-world penetration testing deliverable.

## EDUCATION

**B.Tech in Computer Science and Engineering**, Nirma University (GPA: 8.35 / 10) Present
Ahmedabad, India

## PROJECTS

**L.E.A.P. - Linux Enumeration and Persistence Framework v1.1.0** Link Mar '26

- Designed and built a modular, stealthy Bash framework for post-exploitation enumeration, privilege escalation vectoring, lateral movement, and C2 exfiltration on Linux systems.
- Reconnaissance module: collects kernel version, OS configuration, environment variables, available interpreters, and active shell accounts.
- Enumeration module: identifies SUID/SGID binaries, writable critical paths, Linux capabilities misconfigurations, exposed SSH keys, and credential leaks in Bash history files.
- Network auditing module: maps listening services, active sockets, ARP caches, egress port availability, and dynamically generates reverse shell payloads in Bash, Python, and Netcat.
- Container context module: detects Docker, LXC, and Kubernetes runtimes and evaluates privileged escape vectors via CapEff, host socket mounts, and exposed environment secrets.
- Exfiltration module: compresses in-memory loot stored in /dev/shm and streams it asynchronously to a remote C2 server via Netcat or curl.
- Stealth cleaning module: removes attacker IP from authentication logs, trims Bash history, restores original file timestamps, and shreds temporary artifacts.

## ACHIEVEMENTS & CTF COMPETITIONS

**AWS Skills to Job CTF** Mar '26
Ranked 125th globally and 35th regionally, solving 20 out of 37 challenges across Web Offensive, Forensics, and Mixed Offensive categories. Awarded a 6-month SANS SkillQuest subscription for competition performance.

**TryHackMe**
TryHackMe Jan '26
Ranked in the top 5% globally. Completed the Jr Penetration Tester learning path, covering Metasploit, Burp Suite, network exploitation, web application attacks, and Linux privilege escalation.

## CERTIFICATIONS

**Introduction to Cybersecurity**, Cisco Networking Academy — May '25
**Networking Basics**, Cisco Networking Academy — Jun '25
**Ethical Hacking**, NPTEL — Nov '25