# Rehan Shafiq

+92 301 6567902 | in/rehanshafiq11 | rehanshafiq.infosec@gmail.com | Rehancodecraft | Portfolio

## Education

**Bachelor of Science** — **COMSATS University Islamabad** — *Sahiwal, Pakistan* — **Feb 2024 - present**

- Major in Software Engineering

## Relevant Experience

**Cybersecurity Job Simulation — Deloitte (via Forage)**

- Dug through a 2,000+ line web server log to investigate a simulated breach, and caught a hijacked session by spotting millisecond-exact activity replication alongside a bot hitting the API every hour for over 24 hours.

**Cybersecurity Job Simulation — Commonwealth Bank (via Forage)**

- Triaged web application security issues and worked through log analysis in Splunk inside a simulated bank security-operations environment.

**Shields Up: Cybersecurity Job Simulation — AIG (via Forage)**

- Worked through incident triage and risk assessment for a simulated global insurance enterprise.

## Hands-On Security Practice

- Runs full recon on targets: subdomain enumeration, OSINT, and Nmap-driven port scanning to map what's exposed.
- Scans web apps and networks for vulnerabilities, cross-checking findings against known CVEs to find real risks.
- Built a custom Windows 11 payload that cracked the target machine, giving full Meterpreter access to files, processes, and credentials.
- Comfortable with Kali Linux, Ubuntu, Windows, Python, Bash, SQL, Nmap, Wireshark, Burp Suite, core protocols, and concepts like IDS/IPS, firewalls, Zero Trust.
- Applies this recon-to-exploitation workflow to bug bounty hunting and pentesting on live web apps.

**TryHackMe — Top 8% Worldwide | tryhackme.com/p/rehanshafiq**

- Pre-Security Path (completed): networking fundamentals, Linux basics, web fundamentals, how the web actually works.
- Cybersecurity 101 (in progress): defensive security, OSINT, networking for security, cryptography basics.

## Projects

**VulnScan Tool | Github**

- Scans a target range for live hosts, enumerates open ports/services/versions/OS, and correlates each detected service against the NVD for known CVEs, generating a tabular HTML report.

**Reconnaissance Tool | Github**

- Automated OSINT tool that maps a target domain's live subdomains, open ports, IP addresses, CDN/firewall setup, and technology stack into a formatted PDF report.

**Port Scanner | Github**

- Python-based, multithreaded port scanner using socket programming to detect open ports and service banners on target hosts.

## Achievements & Certifications

- CEH v13 (Certified Ethical Hacker) — exam completed, certification pending
- Google Cybersecurity Professional Certificate — Google, 2026
- Introduction to Cybersecurity — Harvard University (CS50), 2025
- CS50: Introduction to Computer Science — Harvard University (edX), 2025
- Introduction to Networking — NVIDIA, 2025

## Volunteering Experience

**Management Team Member — Notion Society, COMSATS University Islamabad**

- Organized university events for 300+ students, building leadership and project-coordination skills along the way.