JOB DESCRIPTION – SECURITY ANALYST (RED TEAM)

About HackIT

HackIT Technology and Advisory Services is an IT/Cyber Security company, operating since 2009. HackIT is an Indian Computer Emergency Response Team, CERT-IN (www.cert-in.org.in) empaneled provider for IT Security Audit Services. HackIT provides a broad range of security consulting and advisory services to a diverse group of clients, including government organizations, corporations, Military establishments, financial institutions and start-up, to name few. Our work spans multiple sectors and industries, including Telecommunications, Defense and Military, ITeS, Financial Services, Aviation, Hospitality, Healthcare and Research. We work end-to-end—from diagnosis to delivery of lasting impact — together generating tangible results that are improving the security posture of organizations worldwide.

Job Title	• Security Analyst (Red Team)
Location	• Delhi

Job Overview

We are looking for a detail-oriented Security Analyst (Red Team) to join our Security Testing team. In this role, you will lead and execute advanced red team assessments, identify vulnerabilities across applications and infrastructure, and develop clear Proof-of-Concepts to demonstrate security risks. You will collaborate closely with security experts, guide junior analysts, and ensure high-quality reporting and timely delivery of engagements.

Job Responsibilities

- Deliver Red Team exercises and advanced penetration testing across web, network, and endpoint environments.
- Perform manual and automated security testing of Web, API, and Mobile applications.
- Conduct static and dynamic testing (SAST & DAST) of thick clients and applications.
- Develop Proof-of-Concepts (PoCs) for identified vulnerabilities and provide remediation guidance.
- Plan and execute security testing projects with metrics to assess organizational security posture.
- Prepare detailed security reports with findings and actionable recommendations for clients.

Technical Skillsets (Mandatory)

- Write offensive security software such as: backdoors, keyloggers, password dumpers, spear phishing payloads, and web shells.
- Knowledgeable about the cyber kill-chain, and can demonstrate that he or she can: persist on a machine, escalate privileges, steal credentials and move laterally on other machines.

- Find and exploit vulnerabilities in web applications, network services and enterprise network Infrastructures.
- Write in at least two of the following programming languages: C, Golang, Ruby and Python.
- Experienced and knowledgeable in reading Java, C#, C, PHP, Objective C.
- Experienced with databases: MySQL, PostgreSQL, Oracle.
- Experienced with security tools: Burp proxy, Metasploit, Nessus, Kali, and others.
- Sound understanding of security frameworks (OWASP Top 10, NIST, MITRE ATT&CK).

Technical Skillsets (Preferred)

- Threat Modelling.
- Exposure to DevSecOps and Security Architecture review.

Non-Technical Skillsets

- Estimate project efforts and meet delivery deadlines.
- Communicate effectively and deliver results on time.
- Work independently with minimal supervision.
- Lead technical tasks and engage stakeholders efficiently.

Education & Certifications

- Bachelors in IT or equivalent.
- Industry recognized certifications (Eg: OSCP, CREST, eWPT, GXPN, GPEN, Cloud Certifications and other well acknowledged security certifications) preferred.

Experience

1 to 3 years in Application/Infrastructure/Network Penetration testing or Red Teaming.

Send your updated profiles to **careers@hackit.co.**