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.

We are looking for passionate Information Security Professionals to help us keep growing. If you're excited to be part of a winning team, HackIT Technology & Advisory Services is a perfect place to get ahead.

Job Title	• Security Analyst (Red Team)
Location	• Mumbai
Job Overview	• We are seeking a Security Analyst (Red Team) to join our dynamic Security Testing dream team and take lead in performing red teaming assessments. • Hands-on role that also requires oversight and collaboration with team of security analysts.
Job Responsibilities	• Deliver Red Team Exercises • Conduct state-of-the-art penetration testing against web applications, network infrastructures, user workstations, network appliances and other devices and technologies. • Manual and automated security testing of Web applications, APIs, and Mobile Applications. • Static and Dynamic testing (SAST & DAST) of thick clients / applications • Develop Proof-of-Concept (PoC) for the identified vulnerabilities. • Provide remediation guidance to identified vulnerabilities. • Develop and execute security testing project plans. • Incorporate metrics providing comprehensive insight about the security posture of an organization that will help senior management with decision making.

- Write in-depth security report detailing your findings, including advisements on how to remediate the vulnerabilities to the client

Technical Skillsets (Mandatory)

- Write offensive security software such as: backdoors, keyloggers, password dumpers, spear phishing payloads, and webshells
- 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 milestones and deadlines
- Excellent and effective report writing and verbal communication skills
- Deliver results within stipulated time-lines
- Team Player with good interpersonal skills
- Should be able to work independently with minimum and least supervision in complex, dynamic and challenging environment.
- Self-driven and self-managed technical team leader.
- Communicate project requirements and influence stakeholders with minimal supervision.

Education and Certifications

- Industry recognized certifications (Eg: OSCP, CREST, eWPT, GXPN, GPEN, Cloud Certifications and other well acknowledged security certifications) preferred

Experience	• 1 to 4 years in Application/Infrastructure/Network Penetration testing or Red Teaming.
Info Sec Community Activities and Opportunities • romote security researches that are aligned with the	current industry requirements and incepted at HackIT. • Provide assistance and support for presentingresearch papers at security conferences across the globe • HackIT provides opportunity to contribute back to the information securitycommunity

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