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	• Delhi
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. • 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.
Knowledge of:	• Cyber kill chain, MITRE ATTACK Framework, TIBER • Active Directory architecture, policies, and security mechanism • AD attack techniques, such as Kerberoasting, Pass-the-Ticket, Golden Ticket attacks, etc.

	• Network protocols and services, identification of vulnerabilities and potential attack vectors, defenders' response, and bypass. • Techniques for maintaining access and persistence on compromised systems. • Firewalls, IDS/IPS, and other network security controls to navigate through them during attacks
Required Skillsets	• Phishing campaign assessments and tools (Gophish, Evilginx3 etc). • Adversary simulation using C2's like Cobalt Strike, BruteRatel, Sliver etc. • Expertise in Red Team Infrastructure setup and management. • Strong understanding of Cloud Environments and Security (AWS, GCP, Azure). • Scripting for Automation & Security Risk Analysis. • Proficiency in IAC tools (Terraform, Ansible etc.) • Proficient in PowerShell scripts for various tasks, including reconnaissance, privilege escalation, and lateral movement within AD. • Familiarity with Exploitation Frameworks like Metasploit, Core Impact, etc. • Working knowledge of c2 frameworks like havoc, mythic, cobalt strike etc. • Familiarity with tools like BloodHound, PowerSploit, Mimikatz, CrackMapExec, and others commonly used for AD exploitation.
Education and Certifications	• • OSCP (Offensive Security Certified Professional) • OSCE (Offensive Security Certified Expert) • CRTP (Certified Red Team Professional by eLearn Security) • CTP (Cracking the Perimeter by Offensive Security)
Experience	• Minimum 2 to 4 years' experience.

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