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	• New Delhi

Job Overview

We are seeking a detail-oriented Red Team professional to conduct Red Team exercises and advanced penetration testing across applications, networks, endpoints, and devices, including web, API, and mobile platforms, while developing PoCs, simulating real-world attacks, providing remediation guidance, and delivering actionable security reports.

Job Responsibilities

- Plan and deliver Red Team exercises simulating real-world attack scenarios.
- Conduct advanced penetration testing across web applications, network infrastructures, user workstations, network appliances, and related technologies.
- Perform both manual and automated security testing of web applications, APIs, and mobile applications.
- Develop proof-of-concepts (PoCs) for identified vulnerabilities to demonstrate risk and impact.
- Provide clear and actionable remediation guidance for identified security issues.
- Develop and execute security testing project plans in alignment with business and security objectives.
- Define and incorporate security metrics that provide comprehensive visibility into the organization’s security posture and support senior management decision-making.
- Prepare and deliver detailed security assessment reports outlining findings, risk impact, and recommended remediation actions for clients.

Technical Skillsets (Mandatory)

- Experience in phishing campaign assessments and tools such as GoPhish, Evilginx3, and similar frameworks.
- Hands-on expertise in adversary simulation using Command-and-Control (C2) frameworks including Cobalt Strike, Brute Ratel, Sliver, Havoc, and Mythic.
- Strong experience in Red Team infrastructure design, setup, and management.
- Solid understanding of cloud environments and security controls across AWS, Azure, and GCP.
- Proficiency in scripting for automation, security testing, and risk analysis.
- Hands-on experience with Infrastructure as Code (IaC) tools such as Terraform, Ansible, or equivalent.
- Strong PowerShell scripting skills for reconnaissance, privilege escalation, lateral movement, and Active Directory exploitation.
- Familiarity with exploitation frameworks such as Metasploit and Core Impact.
- Practical experience with Active Directory attack tools including BloodHound, PowerSploit, Mimikatz, CrackMapExec, and similar utilities.

Technical Skillsets (Preferred)

- Strong understanding of the Cyber Kill Chain, MITRE ATT&CK Framework, and TIBER methodology.
- In-depth knowledge of Active Directory architecture, group policies, and security mechanisms.
- Hands-on experience with Active Directory attack techniques such as Kerberoasting, Pass-the-Ticket, Golden Ticket, and related methods.
- Solid understanding of network protocols and services, identification of vulnerabilities, attack vectors, defender response, and bypass techniques.
- Experience with persistence and access-maintenance techniques on compromised systems.
- Practical knowledge of firewalls, IDS/IPS, and other network security controls, including techniques to evade or bypass them during Red Team engagements.

Education & Certifications

- Bachelor's degree in IT or equivalent.
- 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

2 - 3 Years experience.

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