

## JOB DESCRIPTION – SECURITY RESEARCHER – WINDOWS

### 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](http://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.

- |                  |   |
|------------------|---|
| <b>Job Title</b> | <ul style="list-style-type: none"><li>• Security Researcher - Windows</li></ul> |
| <b>Location</b>  | <ul style="list-style-type: none"><li>• New Delhi</li></ul>                     |

### Job Overview

We are seeking a detail-oriented security professional to design and develop Red Team and penetration testing tools, primarily for Windows environments, while conducting security assessments, developing vulnerability PoCs, monitoring attack surfaces, delivering client capacity-building services, and recommending security improvements based on emerging threats and industry trends.

### Job Responsibilities

- Design and develop tools for Red Teaming, Penetration Testing, and Security Assessments.
- Perform security testing of Windows systems, web apps, servers, networks, and infrastructure.
- Identify vulnerabilities, develop PoCs, and provide actionable remediation recommendations.
- Build Windows and web-based tools to support Red Team operations.
- Monitor threats, analyze attack surfaces, and deliver client capacity-building services.
- Stay updated with emerging security trends and technologies.

### Technical Skillsets (Mandatory)

- Malware development & Reverse Engineering.
- In-depth knowledge of EDR Evasion tactics.
- Proficiency in development of custom tools for Windows (C, BOF, C#).
- Exceptional Communication and Collaboration abilities.
- Working knowledge of programming in C/C++, Rust, Golang, rust, nim and C# with proficiency in at least one.

- Creation of Malicious Macro Enabled Documents for red team activities.
- Tools such as IDA Pro, OllyDbg, and Ghidra for disassembling and debugging malware.
- Knowledge of scripting languages (Python, PowerShell) to automate tasks and analyze malware samples.

### **Technical Skillsets (Preferred)**

- Windows and Linux OS internals.
- Windows Internals and API (PE, loaders, dlls, hooking, drivers, kernel, and user space, syscalls, IPC) AVR and EDR detection essentials.
- Encryption and cryptographic algorithms to analyze how malware may use them to protect communication or hide its functionality.
- Techniques for maintaining access and persistence on compromised systems.
- Essentials of Firewalls, IDS/IPS, and other network security controls to navigate through them during attacks.
- TTPs in red team operations and defense response and bypass.
- In depth knowledge of C/C++ or C#.
- Static Analysis - Skill in dissecting and understanding malware code without executing it.
- This involves examining the binary code, file structure, and embedded resources.
- Dynamic Analysis - Ability to analyze malware behavior in a controlled environment using sandboxes and virtual machines.

### **Education & Certifications**

- Bachelor's degree in IT or equivalent.
- Relevant Certifications include OSEP/OSED/CRTO II/OSCP

### **Experience**

3 to 4 Years experience.

Send your updated profiles to [careers@hackit.co](mailto:careers@hackit.co)