JOB DESCRIPTION - DEVELOPER - 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) 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
- Developer - Windows

Location
- Delhi

Job Overview

We are seeking a detail-oriented Developer - Windows to perform in-depth security testing, develop Red Team tools, create PoCs, analyze threats, and provide actionable recommendations to improve Windows system and network security. The role also involves client interactions, capacity-building, and staying updated on emerging security trends.

Job Responsibilities

- Perform advanced security testing and Red Team operations on Windows environments.
- Develop and maintain custom Red Team tools, payloads, and Proof of Concepts (PoCs).
- Conduct malware development, analysis, and reverse engineering for research and simulation
- purposes.
- Design and execute EDR/AV evasion techniques to assess defensive capabilities.
- Perform static and dynamic malware analysis using industry-standard tools and frameworks.
- Identify vulnerabilities and provide actionable remediation recommendations to improve system
- and network security.
- Simulate real-world cyberattacks to evaluate detection and response mechanisms.
- Collaborate with internal teams and clients to understand requirements and deliver security
- solutions.
- Prepare detailed technical reports and documentation for stakeholders.
- Stay updated with the latest cybersecurity threats, tools, and attack techniques.
- Support capacity-building initiatives, including knowledge sharing and mentoring junior team
- members.
- Assist in developing automation scripts and frameworks to enhance security testing efficiency

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.
- OSCP (Offensive Security Certified Professional).
- Relevant Certifications include OSEP/ OSED/ CRTO II.

Experience

1 to 3 years’ experience.

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