Rohit Sehgal

OSCP - [verify] · M.Tech · Security Engineer · Researcher

(+91) 9557-56-2015 | rohitsehgal1994@gmail.com | rs@rsehgal.in | rsehgal.in | r0hi7 | r0hitsehgal | @sehgal_rohit

Summary

A **Security Engineer**, who is **OSCP** certified, **Masters degree from IITK** with specialization in System Security and **around 4** years of professional security experience, across **Development of security services**, **Penetration Testing**, **SecOps**, **System Security**, **SSDLC** and **Security Architecture**. Experience in writing Checkmarx SAST Audit Queries. Experience working with SAST & DAST tools. Currently Cybersecurity Engineer at Visa.

A proud Author, Engineer, Maintainer, and architect of extremely reliable and privacy friendly hosted disposable email service **TrashEmail** & Runtime docker security scanning tool **DockerENT**. Authored a book and delivered various security sessions at International conferences. **Inventor of 2 Patents** and **1 Trade-secret**. An active open source contributor.

Work Experience

Visa

Jun. 2019 - Present

Cybersecurity Engineer — *India*

- Invented a **patent and trade-secret** with Visa.
- Experience in writing **Checkmarx SAST Audit Queries**.
- Develop processes and implement tools and techniques to perform ongoing security assessments of the environment.
- Analyze security test results, draw conclusions from results and develop targeted testing as deemed necessary. Also perform secure design reviews as required and provide necessary feedback.
- Led, designed and implemented a project for internal IAM application which helps in tracking **UAR** (User access review) from end to end. Microservice architecture based on Java Springboot and Springcloud, with CI/CD automation using Jenkins.
- Automated various scanning and reporting flows with Python.
- Delivered various security trainings across various product development teams.

Walmart Labs

Aug. 2017 - Jun. 2019

Security Engineer — *India*

- Invented a **patent** with Walmart.
- Work with internal teams to perform penetration tests on their staging operating systems, Network setups and Applications as necessary.
- Hold various workshops and CTFs to better understand state of art exploitation technique and how to mitigate them for product development teams. The highlighted of them were: **Linux System Hardening** & **System Binary exploitation** and was also awarded for the same.
- Responsible for performing manual penetration testing and communicating findings to both Business and Developers, also help them to mitigate the issues.
- Provide guidance to development teams as SME for security as and when required.
- Work with development teams to validate, assess, understand root cause and mitigate vulnerabilities.
- **File Integrity Monitoring** that scales to 50K nodes few of which were legacy nodes.
- Administration portal for controlling Torbit CDN rules. Responsible for entire end to end design of this project.
- **Public Cloud monitoring solution** to continuously monitor public cloud deployments eg Azure and GCP under Walmart's subscription and then generating alerts using Splunk SIEM.

Cybersecurity Research labs, IITK

Jun. 2017 - Jul. 2017

Intern — *India*

- Worked for finding various security flaws at protocol level of industrial SCADA system.

SAMSUNG Research Institute, Delhi

Jun. 2016 - Jul. 2016

Intern — *India*

- HoneyClient Model for smart devices.
- ClientPot for the analysis of the website that are most commonly visited by the user running a smart device.
- The results offered by the system was promising and the system can be slightly modified run on any Linux based devices.

Publications, Talks, & Open Source Projects

Patents

2020 **VISA,** System for Detecting Malicious Changelog Modifications with **Blockchains** — *India, US*

2018 **Walmart Labs,** System and Method of Identifying Malware Compromises in Computing Device — *India, US*

Publications

2020 **Springer,** Honeypot Deployment Experience at IIT Kanpur, Cybersecurity in India

2017 **IITK,** Tracing Cyber Threats with Honey-systems

Talks

2020 **YASCON**, DockerENT: Scanning security mis-configurations for running containers *YASCON, Virtual*
2020 **AppSecIL, OWASP**, Securing Docker containers with DockerENT *Israel*
2020 **GrayHat**, DockerENT: The Only open source tool to scan running containers. *RedTeamVillage*
2020 **RootCon**, DockerENT: Runtime Docker security scanning tool *Vietnam*
2019 **LASCON**, Blockchains for centralised DB systems *Austin, Texas, USA*
2019 **C0C0N**, Cloudmarker: Opensource Cloud monitoring Framework *Cochin, India*
2019 **Defcon DC-0471 - 0x3**, Capturing Insider threats using Blockchains *Trivandrum, India*
2018 **Defcon DC-0471 - 0x2**, HoneyTraps to capture mobile device Malware breaches *Trivandrum, India*
2017 **Walmart Labs**, Linux Binary Exploitation *India*

Blogs

2020 **DevOps Community**, Learn Kubernetes in Just 30 Mins *GitHub*
2018 **Medium Blog**, Splunk — Shall we begin ? *Medium*
2017 **Walmart Labs Tech Blog**, Additional auth to Django admin login *Medium*
2017 **Security Community**, Linux Binary Exploitation from Scratch *GitHub*

Open Source Projects

2020 **Python**, DNS Over TLS Proxy *GitHub*
2020 **Python**, DockerENT: Runtime Docker security scanning tool *GitHub*
2020 **Java**, TrashEmail: A disposable email service. *GitHub*
2020 **Java**, Telegram Connector plugin to connect a bot to REST service. *GitHub*
2019 **Python**, CloudMarker: An Open source cloud monitoring framework. *GitHub*
2017 **C, C++, Python**, BinExp: Understanding program corruption. *GitHub*

Skills

- **Web Application Security**
- **Reverse Engineering**: Buffer Overflows, ASLR bypass, Executable stack, ShellCode Execution, GOT, ROP, Format Strings, Heap Overflows etc.
- **Security Tools**: Metasploit, Msfvenom, nmap, hashcat tcpdump, SAST, DAST and lot of other tools that comes with KaliOS etc.
- **Programming Languages** I am comfortable building applications with: **Java, Python, C/C++**.
- **DevOps**: Docker, Docker Compose, Docker Swarm, Kubernetes, Jenkins, Git.
- **Frameworks**: Spring-Boot, Spring-cloud, Django.
- **Applications** I love to play with: Linux CLI and Mac CLI & VIM.

Awards

2020 **VISA**, Star of Quarter: Cybersecurity
2018 **Walmart Labs**, Recognition on a global platform
2017 **IITK**, SIDBI Incubation Center, IITK(SIIC) for the Student Innovation Award.
2017 **IITK**, Innovative Project Award, Across the batch of 2017.
2016 **IITK**, Honorarium for successfully teaching System Security Course at IITK.
2015 **BTech**, GOLD medal for Best performance.
2015 **IOCLS**, Recipient of **Indian Oils Merit Scholarship**, Scholar No **11210212**

Education

Indian Institute of Technology, Kanpur *India*

M.Tech CSE, With Specialization in System Security *Jul. 2015 - Jun. 2017*

- **Awarded Best Innovative Thesis**.
- CGPA: 8.3
- Proposed and implemented set of effective honeypot models to capture threats for various services ranging from ssh service to service for mobile devices. The implemented system was successfully identify threats in the smart way. The results had helped IITK to build an secure infrastructure. The implemented set of systems are further studied by the other graduating students for the base of their M.Tech Thesis
- Proposed and implemented a Honey Token model for capturing mobile device breaches by hidden malware.