

Mohit Balu

Persistent, detail oriented, IT professional experienced in Enterprise Vulnerability Management. Capable of handling critical assessments along with project management in a busy corporate environment. Proficient in liaising with IT professionals, performing timely deliveries and working in a collaborative environment while maintaining customer focus for better business operations.

✉ mohit.balu@outlook.com

📞 +1 (514) 754-0755

📍 Montreal, Quebec

🌐 [linkedin.com/in/mohit-balu](https://www.linkedin.com/in/mohit-balu)

WORK EXPERIENCE

Cyber Security Analyst

Tata Consultancy Services – Bhubaneswar, India

Jul 2019 – Jan 2022, India

Roles and Responsibilities

- Conducted vulnerability assessment & penetration testing on web applications, internal & external network infrastructures and prepared reports which documented security risks and related extent of damage.
- Worked with customers to implement system security measures, assisted them with technical guidance on remediation of vulnerabilities.
- Developed various automated scripts in python to assist the team in improving vulnerability assessment process during security assessments.

EDUCATION

Master of Engineering in Information Systems Security

Concordia University, Montreal

Jan 2022 – Jun 2023

GPA: 4.1/4.3

Bachelor of Technology in Computer Science

Lovely Professional University, Phagwara, India

Aug 2015 – May 2019

GPA: 9.2 (82.8%)

Engineering Minor in Cyber Security

PUBLICATIONS

Review Paper

Security Techniques in Vehicular Ad hoc Networks

<https://bit.ly/vanets-review-paper>

Authors: Mohit Balu, Gulshan Kumar, Se-Jung Lim

International Journal of Control and Automation, Apr 2019

A review paper on different security techniques being used in a vehicular ad hoc network to protect Intelligent transport system from emerging security threats. Published in Scopus indexed journal with five citations.

CERTIFICATIONS

- Professional Cloud Security Engineer (Google Cloud) Sep 2021
- EC-Council Certified Ethical Hacker v10 Feb 2019
- Cisco Certified Entry Networking Technician Dec 2017

Network and Application Security

Penetration Testing

Vulnerability Management

Python Scripting

Red Teaming

Container Security

Advanced Excel

CONFERENCES

Security BSides, Montreal

Sep 2022

NullCon Security Conference – Advanced Infrastructure Security Assessment (Online)

Mar 2021

Feynman 100 – International Conference on Computing Sciences, LPU, India

Aug 2018

ACHIEVEMENTS

Star of the Month Award (Apr 2021)

Received Star of the month award at TCS for hunting down exceptional vulnerabilities in customer's network infrastructure.

Special Initiative Award (Dec 2020, Feb 2021, Sep 2021)

Received special initiative awards for outstanding contribution in business CTF at Hack the Box and at other occasions at TCS.

Cisco Netriders Competition (Sep 2017)

Achieved 2nd rank in India and 32nd in Asia Pacific & Japan Region in Cisco Netriders Competition.

VOLUNTEER POSITIONS

Vice President – CyberHack Student Club, LPU, India

Sep 2018 – Jul 2019

- **Roles:** Organize and deliver cyber security workshops, invite speakers, arrange learning content for members.
- **Skills Learned:** Leadership, Teamwork, Time management.

PROJECTS

- **Implementation of Virtual Network inside Cloud Environment using OpenStack with an IDS for attack detection** Jul 2022
<https://github.com/cyc0rpion/INSE6620-Project>

Demonstrated a multi-node OpenStack cloud environment, running a web application along with Snort Intrusion Detection System inside a virtual private network. The scenario was composed of following components:

- 2 Virtual Private Networks, for both attacker and the victim.
- 3 Virtual Linux instances, for hosting web application, Attacker's system, and Snort machine

Following attacks were implemented and simulated for detection:

- TCP SYN Flooding attack
- Malicious FTP Login attack

- **DockerSec - Simulated attacks and their prevention on a containerized environment** Apr 2022
<https://github.com/INSE6130-Project/Docker-Security>

Demonstrated recent attacks implementation and execution on Docker environment, including but not limited to:

- Gaining initial foothold through broken authentication
- Misusing discovered sensitive information
- Exploiting unprotected docker socket
- Abusing excessive capabilities
- Exploiting known vulnerabilities
- Misusing missing signature verification

Implemented security mechanisms using Python to detect and prevent above listed attacks, by:

- Scanning image manifests to detect sensitive information
- Docker socket detector and capabilities checker
- Registry authentication and signature implementation
- IP Based filtering

- **Open Forensics Toolkit** Nov 2018
<https://github.com/cyc0rpion/DeCryptoSuite>

Developed a python toolkit to solve steganography, cryptography, and forensic challenges in capture the flag events. Following five modules were developed to build a complete toolkit:

- Cryptanalysis
- Steganalysis
- Optical character Recognition
- Disk Imager
- Log Extraction