Divya Goswami

Versatile Operational and Security engineer with experience in system administration, site reliability, automation and programming. Capable of working under any environment.

Edgbaston, Birmingham
mail@rachejazz.me
Portfolio link: https://rachejazz.me
Github Profile: https://github.com/rachejazz
Tech Blogs: https://rachejazz.me/blogs.html

Education

University of Birmingham
MSc in Cybersecurity
2023 - PRESENT , BIRMINGHAM
Aced modules:
Cryptography and Network Security,
Forensics, Malware and Penetration Testing

Heritage Institute Of Technology
Btech in Computer Science
2018 - 2022, INDIA, CGPA 8.2/10
Aced modules:
Year 2: Operating Systems,
Year 3: Database Management Systems and
Year 4: Cryptography and Network Security

Skills

Security Researching:
- Analyzing windows malware using **Ghidra/Cyberchef**
- Dynamic analysis using **FlareVM** and **Remnux** tools including **procmon/x64debug**

Scripting and Automation:
- Scripts using **Bash** and **Python** over **AWS** and **GCP** and cicd over **Jenkins**

Demonstrate expertise in the knowledge of **GitSecOps**.

System Administration:
- Efficient both on **Linux** (5yrs) and Windows servers.
- Compete over challenges on **hackthebox/vulnhub** and prepare for **OSCP** certification.
- **Kubernetes Monitoring** and **Security. Secret Management, cluster hardening** based on CISA rules.
- Hardening **Docker** images and setting up healthchecks for failed pipelines.
- Custom building **Linux kernel**, creating drivers in **C**
- Configuring **Network Firewalls, Security Scanners**, conducting **VAPT** reports on product

Projects (All available on github)

- Reverse windows malware on Ghidra
- ARM code emulation using unicorn emulator on python
- Bypassing CSP, File Forensics a study of how polyglot files can be taken advantage of in bypassing CSP rules for Reflected XSS attacks.
- Deployment using Voice assistant driven pipeline
- Laufeyson, Domain Recon Framework capable of gathering intel on a domain or an IP.
- Study of the GNU toolchain for InterProcess Communication(IPC) in an OS
- Software simulation of a computer from scratch.
- DevSecOps-Automation-Monitoring scripts that can be used for daily workflows.
- Keka Reminder Bot capable of sending scheduled messages with minimal memory consumption.
- New Tab Extension that supports chrome and firefox browsers. Available on Firefox Add-ons.

Employment

- **Site Reliability Engineer**
  June 2022 - August 2023
  Workspan, Angad Corporate, Pvt, Ltd.
  - Automation in GCP to Jira Integration, open firewall detection and removal, expired IAM access purging
  - CICD security scanning, SCA, SAST, DAST report creation.
  - Google Security Command Centre exploration and instructing strict adherence to security practices.
  - Secret Management, SSL certificate update, WAF configuration on GCP

- **DevOps Intern**
  March 2022 - June 2022
  INDmoney, Finzoom Investment Advisors (P) Limited.
  - Setting up metrics and alerts for RDS/ECS Services/Redis clusters using cli and setting up dashboard on grafana by linking cloudwatch logs using arn policy.
  - Recording data of uncharted resources over excel sheet using 100% automated workflow.
  - Tag based cost allocation and migrating cost exploration from AWS to Grafana. Setting up Jenkins job for auto allocation of tags of every new resource
  - Assigned with core deployment window. Issuing hotfixes and monitoring proper GitOps deployment everyday.

- **Dev(Sec)Ops Intern**
  September 2021 - March 2022
  Trell Experiences Pvt Ltd.
  - Implemented GitOps Security - access control, CI/CD pipeline upgrade
  - Docker and Kubernetes Security - Deployed Vault and Falco via helm for secret rotation and management and monitoring events on k8s cluster. Created hardened Docker images for restricting privileges to running services.
  - System-Admin, Security and IAM - Created scripts to scan unprivileged users using sudo on server, on demand log monitoring based on time period over kibana, automate exit policy for employees exiting the org.

- **Open Mainframe Project Mentee'21**
  June2021 - Aug 2021
  The Linux Foundation, IBM Z
  - Revamped a Flask application for IBM Z
  - Refactored 70% of code and improved UI and Backend.
  - Scripted automations for pulling and formatting data for various Linux Distributions.
  - Reduced 80% manual configging and reloading of server that helped moving forward with CI/CD Pipeline

- **Jr. DevOps Engineer**
  Dec 2020 - Feb 2021
  Dynopii Pvt. Ltd.
  - Administered 4 Linux servers
  - Surveillanced application deployments on Digital Ocean.
  - Wrote Dockerfiles and docker compose and tested deployment locally on VMWare.
  - Setup fail2ban firewall for preventing online VoIP server attacks.

Achievements

- Student Ambassador, Msc CyberSecurity 2023
- AWS Community Builder 2022
- IBM Z Ambassador 2021
- GHC Scholar and OpenSource Mentor 2021
- Scholarship to Attend BlackHat Europe 2023
- Beginner in Linux Kernel Development 2022
- Linux Server Management and Security 2022