

Lakshya Rao

Developer | Pentester | Cyber Security | CEH | SOC

EXPERIENCE

Sify Digital, Noida — Security Engineer

JUN 2022 - Present

On-site: Punjab National Bank, Sansad Marg, Delhi.

- **Security Information And Event Management (SIEM)**
 - **RSA Netwitness:**
 - Monitoring Logs for Threat Hunting
 - Monitoring Dashboards
 - Creating and Customizing Reports as per client requirements.
 - Creating Filters to fetch relevant Logs
 - Correlating Security Events on Different Security Devices.
 - Making rules to prevent ongoing or upcoming threats
 - Backup and CLI Management (RHEL)
 - Mitigating Vulnerabilities as per VA Report.
 - Raising Security Incidents, Maintaining Incident record and Closing Incidents as per SLA.
 - Mitigating vulnerabilities as per VA report
 - **ArcSight:**
 - Monitoring Logs on ESM and Logger for Threat Hunting.
 - Making Filters to Get Relevant logs.
 - Making Customized Dashboards for Better Visibility over Security Devices.
 - Making Customized Query, Trends and reports as per client's requirement.
 - Making Active Channels on ESM
 - Making Rules and alerts on ESM to prevent ongoing and upcoming threats.
 - Raising Security Incidents, Maintaining Incident record and Closing Incidents as per SLA.
 - Integration and Implementation on Both Windows and Linux platforms.
 - Mitigating vulnerabilities as per VA report.

🏠 47-A, Shri Sai Apartment,
Sector -71, Noida (U.P)

☎ (+91) 99112-31585

✉ lakshyarao22@gmail.com

🌐 <https://theinquisitive.xyz>

CYBER SECURITY

SIEM: RSA Netwitness, Micro Focus Arcsight, Micro Focus Fusion.

WAF: Radware Apsolute vision.

NBAD: Cisco StealthWatch.

VAPT: Tenable Nessus, OpenVAS, Nmap, Metasploit.

HONEYPOT: Zscaler Deception.

VM: VMware vSphere, QEMU, VIRTmanager.

FW-MGMT: Skybox Security.

OS: Windows, Mac OS, Open BSD, Linux (Arch, Ubuntu, Debian, CentOS, RHEL, Kali Linux, ParrotOS).

SKILLS

FrameWork: Flutter, IoT, Android, iOS, Networking, Cyber Security.

Designing: Figma, Photoshop, Inkscape, Illustrator, Gimp.

Tools: Git, Github, Neovim, VS Code.

Hardware: Raspberry Pi, Arduino, ESP32.

- **Web Application Firewall (WAF)**

- **Radware Absolute Vision:**

- Onboarding Servers to WAF
 - Making virtual Services
 - Load balancing on WAF
 - SSL Certificate updation
 - Setting up SSL Offloader
 - Making Security Policies
 - Deep Traffic Inspection
 - Log Analysis and threat Hunting
 - Refinement of policies
 - Configuration Backup and updation of Signatures
 - Upgradation to newer Versions

- **Network Behaviour and Anomaly Detection(NBAD)**

- **Cisco StealthWatch:**

- Creating Host Groups
 - Defining and configuring custom role policies
 - Logs Monitoring and taking proper action towards threat
 - Analysis of alarms
 - Patching, Upgrading to newer versions
 - Backup and other daily operations.

- **Vulnerability Assessment**

- **Tenable Nessus:**

- Creating policies
 - Scheduling vulnerability scans.
 - Creating vulnerability scans
 - Creating VA Report
 - Updating plugins and Patching
 - Managing CLI (CentOS7)
 - Defining and managing all prerequisites for scan.
 - Managing user roles and groups
 - Performing Full vulnerability scan and generating custom report as per clients requirement.

- **Honey Pot**

- **Zscaler Deception:**

- Creating policies
 - Managing Updates and backups
 - Creating Custom Decoys.
 - Integrating VirusTotal and AbuseIPDB APIs
 - Managing CLI (Rocky Linux)
 - Managing user roles and groups
 - Monitoring Dashboard for Threats
 - Integrating Firewall for immediate Containment of threats.

Programming Languages:

Dart, Python, HTML, CSS, Javascript, Embedded C, Bash, C, C++.

CERTIFICATION

- Certified Ethical Hacker
- FreeCodeCamp
- APIacademy: API Designer and security Architect
- Arcsight Fusion Training

LANGUAGES

Hindi (Mother tongue)

English (Fluent)

- **Firewall Management**

- **Skybox Security:**

- Analyzing Firewalls
 - Adding Firewalls to system
 - Creating custom policies for risky ports
 - Creating reports for further analysis
 - CLI Management (CENTOS7)
 - Mitigating Vulnerabilities.
 - Updating and Backups
 - User Management
 - Monitoring for errors and mitigating them.

Virtual Analytics, Noida — *IoT and Development Intern*

OCT 2020 - OCT 2021

- **Smart Attendance System:**

- Built on python and OpenCV Library
 - Uses Artificial Intelligence to detect Faces.
 - Reliable Operation for Office Spaces
 - No-touch required to Avoid spread of COVID
 - Built on RaspberryPi so no external computer Required
 - Low Power Consumption
 - Work in low light
 - Integrated Touch screen for easy management.
 - 3D Printed Case for easy maintenance.

- **Home Automation System(Tatva IoT):**

- Built on reliable ESP32 Module
 - Hub Based so no Internet required
 - Can be integrated with other smart home technologies
 - Based on WIFI for higher range
 - Mobile Application built on Flutter.
 - Works on both iOS and Android
 - Code Written in Embedded C
 - 200 modules can be integrated to single HUB

- **Payments Application(Afriq Pay):**

- Built on Flutter
 - Using Currency Cloud API for international Money Transfer.
 - Using Reloadly API for Mobile Recharge
 - Using Stripe payment gateway for receiving payments.
 - Works on Both iOS and Android

- **E-Commerce Application(BoozDO):**

- Designed on Figma as per clients requirement
 - Developed in flutter for compatibility on both iOS and Android
 - Uses Custom backend built on AWS and node.js

EDUCATION

Ajay Kumar Garg Engineering College, Ghaziabad — *B-Tech(E.E.E)*

JUL 2017 - MAR 2022

I have completed my Bachelors in Electrical and Electronics Engineering.

Kendriya Vidyalaya, Noida — *Intermediate*

APR 2015 - MAR 2017

I have completed my intermediate from Science With Biology.

PROJECTS

Home Automation — *with ESP32 and MQTT*

Used ESP32 and brains of the project and used MQTT to connect it with Alexa and Google Assistant

24/7 Youtube Live Bot — *with ffmpeg and python*

Used AWS to host a Ubuntu instance and used Bash And python to Automate ffmpeg and sqlite to Stream a 24/7 live music Radio.