Rooshan Riaz

Pakistan riazrooshan@google.com 3367095138 rooshanriaz rooshanriaz

Education

Ghulam Ishaq Khan Institute of Engineering Sciences and Technology *Sept 2022 – May 2026*
BS in Cyber Security

- GPA: 3.41/4.0

Experience

DevOps Intern *Remote*
ALNAFI *Nov 2024 – Mar 2025*

- Managed and optimized AWS cloud infrastructure, configuring and deploying EC2, VPC, IAM, S3, RDS, Route53, ELB, CloudWatch, and other services, ensuring efficient cloud operations and cost management.
- Configured and maintained Kubernetes clusters, ensuring optimal sizing, security, and networking. Deployed applications, managed resources, and implemented blue-green, canary, and rolling updates to minimize downtime. Automated infrastructure with Ansible, Docker, and Kubernetes for efficient scaling and load balancing.
- Administered Linux systems, overseeing installation, troubleshooting, user and file system management, networking, and configuring essential servers like FTP, NFS, DHCP, SAMBA, Apache, DNS, and POSTFIX.

Security Intern *Islamabad, Pakistan*
Bytewise Limited *June 2024 – Aug 2024*

- Gained hands-on experience in setting up and hardening Ubuntu Server, implementing OWASP TOP 10 security practices, and configuring Active Directory in Windows Server 2022.
- Developed expertise in CIS Top 20 Controls, performed threat intelligence using ANY RUN, and analyzed network traffic with Wireshark.

Projects

Security Audit *Github Link*

- Conducted a cybersecurity audit by designing a detailed questionnaire distributed to major organizations across Pakistan. Compiled findings into a report outlining security measures, vulnerabilities, and improvement recommendations.

STUDENT MANAGEMENT SYTEM *Github Link*

- Developed a web system with an HTML/CSS frontend and a Flask-based Python backend. Integrated PostgreSQL and Cloud Firestore for data management, supporting three user roles: students, teachers, and administrators.
- **Tools Used:** Python, Flask, Firebase, Postgresql

Azure Chaos Engineering *Github Link*

- Conducted chaos engineering on Azure to assess infrastructure resiliency and security. Automated fault injection via Azure CLI and PowerShell, analyzed system responses, and identified monitoring gaps. Recommended enhancements for robustness and recovery.
- **Tools Used:** Azure CLI, Azure Monitor, Log Analytics, Azure Automation, Azure Storage, Network Security Groups (NSG), KQL (Kusto Query Language)

Technologies

Tools & Technologies: Docker, Flask, Git, CodeQL, Jira, GitHub Actions, Wireshark, Nessus
Languages: Python, Bash, SQL