Rooshan Riaz

0336-7095138 | riazrooshan@gmail.com | linkedin.com/in/rooshanriaz | github.com/rooshanriaz

Education

Ghulam Ishaq Khan Institute (GIKI) Sept. 2022 – June 2026
CGPA: 3.41/4.00
Achievements: Dean's Honor List Fall 2023
Bachelor of Science in Cyber Security

Experience

System Administrator Apr 2024 – Apr 2025
ALNAFI Cloud Karachi, PK

- Administered Linux file systems, including symlinks, hard links, archiving, and compression, to maintain system integrity and data security.
- Administered Linux servers by managing users, configuring FTP, SAMBA, and deploying Apache web services.
- Provisioned AWS infrastructure using EC2, S3, IAM, and VPC for scalable, secure cloud environments.
- Configured TCP/IP networking: static IPs, gateways, DNS, domains, and subnetting to ensure connectivity.
- Implemented Iptables firewall rules to restrict unauthorized access and enforce network traffic security policies.
- Automated recurring administrative tasks with CRON and shell scripting to improve system efficiency.
- Performed kernel patching, tuning, and upgrades to enhance Linux system performance and maintain stability.
- Managed LVM storage to enable dynamic disk provisioning, scalability, and efficient volume management.

Projects

Secure Network Architecture using SDN | *Cisco Packet Tracer, Software-Defined Networking (SDN)*

- Implemented Access Control Lists, VLAN segmentation, and SSH authentication for secure communication.
- Deployed SDN controllers to manage devices centrally for faster configuration and policy enforcement.
- Enabled traffic flow visualization and automated network diagnostics for quick issue detection.

Reddit Clone App on Kubernetes with CI/CD | *Docker, Terraform, Kubernetes, GitHub Actions*

- Built and deployed a containerized Reddit clone using Kubernetes and Docker with full CI/CD using GitHub Actions.
- Automated AWS infrastructure using modular Terraform IaC, ensuring scalable, secure, and repeatable deployments aligned with the AWS Well-Architected Framework.

Forensic Analysis of Ransomware Attack | *Autopsy, FTK Imager, Volatility, PEStudio*

- Leveraged Volatility and Autopsy tools to extract and analyze volatile memory and disk artifacts, reconstructing ransomware infection timelines and data recovery opportunities.
- Conducted static malware analysis with PEStudio and network traffic monitoring using Wireshark to identify ransomware indicators and command-and-control activity.

PhishGuard | *JavaScript, MongoDB, ZAP, Irius Risk*

- Built a phishing detection browser extension with secure JWT authentication and MongoDB backend.
- Performed threat modeling and dynamic security testing using OWASP ZAP to identify and fix vulnerabilities.

Security Audit | *Python, Pandas*

- Performed cybersecurity assessments by creating and distributing structured questionnaires to organizations.
- Analyzed audit responses using Python (Pandas) to assess security posture, identify recurring vulnerabilities, and recommend risk mitigation strategies.

Technical Skills

Cyber Security: Wireshark, Nmap, ZAP, ELK Stack, Snort, Suricata, Autopsy, Volatility, FTK Imager, CodeQL, PEStudio, Sleuth Kit
Software Engineering: Python, Bash, Flask, PostgreSQL, MongoDB
Cloud & DevOps: Docker, Kubernetes, Terraform, GitHub Actions, AWS
Tools: Jira, Git, Postman