Abdulrehman Aman

House No. A-946 Sector 11-B North Karachi, Karachi
Department of Computer Science, University of Karachi, Karachi, Pakistan
+92 334 2451933 | abdulrehman aman | mailto:abdulrehman.aman91@outlook.com| Abdulrehmanaman-91

HIGHLIGHTS

- Final year BS Computer Science student at the University of Karachi with strong interest in DevOps practices and automation**.**
- Hands-on familiarity with Linux administration, Git version control, Networking fundamentals, Docker containerization, and Chef configuration management**.**
- Quick learner with a cybersecurity background, bringing knowledge of SOC operations, SIEM, and security best practices to support secure DevOps workflows.
- Strong analytical mindset with the ability to collaborate in fast-paced environments, ensuring reliability, scalability, and security of systems.
- Gained hands-on exposure to AWS EC2 for deploying and managing Linux-based instances.

CAREER OBJECTIVE

Aspiring DevOps Engineer with a solid foundation in Linux, Git, Docker, Chef, and Networking fundamentals, along with hands-on SOC experience. Currently transitioning from cybersecurity to DevOps with a long-term vision of becoming a DevSecOps professional**,** integrating automation, system reliability, and security best practices into modern development workflows. Seeking a DevOps role to apply my skills in automation, containerization, and secure system administration

EDUCATION

B.Science. in Computer Science — Dec 2021 –Dec 2025
University of Karachi — Karachi, Pakistan

Intermediate in Pre Engineering — Sep 2019 – Oct 2021
Admajee Govt. Science College — Karachi, Pakistan

Matriculation — Mar 2008 – July 2019
Usman Public School System — Karachi, Pakistan

EXPERIENCE

Information Security Analyst, Security Operation Center — Feb 2025 – Sep 2025
Rewterz — Karachi, Pakistan

Monitoring Security Alerts:
- Continuously monitor SIEM dashboards and alert queues for suspicious activities or anomalies.
- Respond to alerts generated by security tools (e.g., SIEM, EDR, firewalls, etc.).

Initial Triage and Investigation:
- Perform preliminary analysis on alerts to determine severity and potential impact.
- Collect basic information (source IP, destination IP, user account, timestamp, etc.) for further investigation.

Use of Security Tools:
- Work with tools such as SIEM RSA NetWitness, EDR, and XDR platforms.
- Understand log sources and contribute to correlation rule tuning

Email and Phishing Analysis:
- Perform initial analysis of suspicious emails and assist in identifying phishing attacks.

Communication:
- Coordinate with team members and other departments during incident handling.
- Provide status updates to senior analysts and follow instructions for deeper analysis or containment.

SKILLS AND CERTIFICATIONS

Cybersecurity Tools; Programming Languages and Technical Environments

- **Programming & Scripting**: Python (automation scripts), Bash scripting for automation and security tasks.
- **Version Control**: Git (branching, merging, CI/CD pipeline integration).
- **Linux Administration**: Hands-on experience with Linux commands, system administration, and troubleshooting.
- **Networking Fundamentals**: TCP/IP, DNS, HTTP/HTTPS, SSH, firewalls, and basic network troubleshooting.
- **Configuration Management & Automation**: Chef (cookbooks, recipes) for automated server provisioning and configuration.
- **Ansible** (basic playbook creation, configuration automation).
- **Containerization & Orchestration**: Docker (image building, container management).
- **Jenkins** (basic CI/CD pipeline setup).
- **Monitoring & Security Tools**: RSA NetWitness (SIEM), EDR, XDR; skilled in monitoring dashboards, alert triage, phishing email analysis, and log investigation.
- **Incident Handling**: Familiar with writing rules, performing initial incident response, and coordinating with cross-functional teams.
- **Phishing & Malware Analysis**: Performed first-level analysis of suspicious emails, identified phishing attempts, and extracted URLs and malicious attachments.

Certifications

- IBM Cybersecurity Analyst: Gained knowledge about cybersecurity tools, compliance, and incident response. Acquired knowledge in threat intelligence, data, and endpoint protection
- Ethical Hacking Essentials (EHE): Learn fundamentals of information security and ethical hacking. Learn about information security threats and vulnerabilities, types of malwares, and vulnerability assessments.
- Metasploit for Beginners: Ethical Penetration Testing: Perform a Vulnerability Scan Analysis to enable effective vulnerability reporting. Utilize an exploit using Metasploit to gain access to a vulnerable system.
- **Digital Forensic and Cybersecurity | NAVTTAC:** Introduction to Cybersecurity Tools & Cyberattacks. Penetration Testing, Incident Response and Forensics. Gained knowledge in areas such as threat detection, incident response and vulnerability assessments.