



CONTACT



+92-03343388474



umarsaad911@gmail.com



www.linkedin.com/in/umar-saad



Karachi, Pakistan

EDUCATION

BS. in Cyber Security

FAST-NUCES

Aug 2020 - May 2024

SKILLS

- Team work and collaboration
- Hands-on exp of digital forensics
- vulnerability assessment
- Incident Response
- SEIM tools like steller cyber/Qradar
- Concept of cryptography
- XDR/EDR

TOOLS

- Nessus
- Wireshark
- Cyberchef
- ZAP OWASP
- Sonar Qube
- Qradar
- Burpsuite
- Nexpose
- Regshot
- AnyRun
- OpenVAS
- MTM

UMAR SAAD

CYBER SECURITY

WORK EXPERIENCE

SOC Analyst Internship

July 2023 - Sept 2023

SUPERNET

SEIM Tool >> Steller Cyber

VAPT Tool: >> Rapid7 Nexpose

Demonstrated in depth knowledge of alert management and analysis Successful deployment of Qradar locally and managed dashboard Hands-on experience on how to generate comprehensive vulnerability reports

Teaching Assistant

FAST NUCES

Aug 2023 - Dec 2023

Fundamentals of Malware analysis

Designed and graded assignment for malware analysis course Provided guidance and assistance to student in their projects

PROJECTS

Real Time Anomaly Detection System

May 2022

python/SQL

monitors the incoming and outgoing packets by parsing the queries through regex comparison and anomaly detection.

Kubernetes Security

Apr 2023

- Deployed EshopOncontainer, a sample reference application by Microsoft, on a Minikube Cluster using Helm.
- Conducted penetration testing and vulnerability scanning with open-source security tools including Kube-Bench, Kube-Hunter, Sysdig, Trivy-Operator, and Kubesecc.
- Implemented ARMO for advanced security, container isolation, and automated application lifecycle management.

ACHIEVEMENTS

5th position in Pakistan first Cyber security challenge (CTF) PCC - 2022
6th position in ignite Cyber security competition (CTF) - 2022
3rd position in Procom'23 Capture The Flag(CTF) competition - 2023
4th position in ignite Cyber security competition (CTF) - 2023

COURSES CERTIFICATION

certification of SOC analyst from (Let's Defend)

Foundation of Cyber Security by google (Coursera)

Practical Ethical Hacking (TCM Security)

Cyber defense (TryHackme)