Arsalan khan

+92-344-7787622 | arsalanswat7@gmail.com | Arsalan Khan | arsal7477 | Portfolio
Ghalegay, Barikot Swat, Pakistan, ZIP Code: 19230

Summary

Eighth-semester Cybersecurity student with hands-on experience in network defense, threat intelligence, and penetration testing. Equipped with practical skills gained through industry internships, academic projects, and leadership roles. Actively seeking opportunities to contribute to security teams in roles involving SOC operations, vulnerability assessment, or security research. Passionate about applying technical knowledge to real-world challenges in a professional environment.

Experience

- **Pakistan Air Force** *July 2025 – August 2025*
  Cyber Security Intern Islamabad, Pakistan
  - Assisted with SOC monitoring, network configuration, vulnerability assessment and penetration testing activities.
  - Performed PortSwigger labs using Burp Suite and conducted end-to-end security testing on a DVWA environment.
  - Delivered tasks reliably while demonstrating professionalism, punctuality, and strong problem-solving skills.
- **ITSOLERA PVT LTD** *July 2024 - September 2024*
  Red Team Intern Remote
  - Conducted penetration testing to identify vulnerabilities and enhance cybersecurity defenses.
  - Designed and developed ConnectFinder, a Python-based People Search Tool that aggregates data from multiple sources, enhancing identity verification and threat analysis.
  - Gained hands-on experience in penetration testing, threat analysis, and security assessment.

Education

- **Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (GIKI)** *September 2022 - Present*
  Bachelors of Science in Cyber Security Topi, Pakistan
  - **CGPA:** 3.43/4.00
  - **Final Year Project:** TrustChain: A Blockchain-based Secure Voting System

Projects

- **Malware Traffic Detection Using Victim-Attacker Interaction Patterns** *Dec 2025*
  Tools: Python, PyTorch, Scapy, LightGBM, Google Colab
  - Built malware detection system analyzing encrypted traffic patterns with 99.88% accuracy.
  - Engineered 22 statistical features from 16-packet channel units using LightGBM.
  - Implemented SampleNorm for traffic non-stationarity, robust to 20% packet loss.
  - Classified 10 malware families with 96.24% multi-class accuracy.
- **End-to-End Vulnerability Assessment System** *Nov 2025*
  Tools: pfSense, Wazuh SIEM, Kali Linux, Python, Suricata, Metasploit, Windows Server
  - Built segmented 3-zone corporate network (External/DMZ/Internal) with pfSense firewall.
  - Identified 34+ vulnerabilities including SQLi, XSS, CSRF; achieved 85% detection rate.
  - Configured Wazuh SIEM with custom rules and Suricata IDS for active defense.
  - Automated CVSS scoring with Python and mapped controls to NIST CSF/ISO 27001.
- **Secure Ride-Hailing Web Application** *Apr 2025*
  Tools: Python, Flask, MySQL, HTML/CSS/JS, Mapbox API, JWT, bcrypt
  - Developed a secure multi-role (user/driver/admin) ride-hailing platform using Flask.
  - Implemented hashed passwords, JWT-based session handling, and CSRF protection for secure authentication.
  - Integrated Mapbox API for live ride tracking and outsourced payments to maintain PCI-DSS compliance.
  - Applied OWASP security practices to mitigate SQL injection, XSS, and other web vulnerabilities.
- **QRGenX: Cloud-Native QR Code Generator** *Mar 2024*
  Tools: Python, Flask, Docker, AWS EC2, Terraform, GitHub Actions, Prometheus, Grafana
  - Built a containerized QR code generation API using Flask and Docker.
  - Deployed the service on AWS EC2 with Auto Scaling Groups provisioned via Terraform.
  - Implemented CI/CD pipelines with GitHub Actions for automated testing and deployments.
  - Configured Prometheus and Grafana dashboards for real-time performance monitoring and alerts.

- **Anomaly-Based Intrusion Detection System (IDS)** *Dec 2024*
  Tools: Python, Google Colab, Pandas, NumPy, Scikit-Learn, Matplotlib
  - Implemented K-Means clustering with PCA to detect anomalous network patterns.
  - Processed and normalized network traffic data with 40+ behavioral features.
  - Achieved a Silhouette Score of 0.87 indicating clear cluster separation.
  - Visualized clusters to highlight abnormal traffic points and deviations.
- **Genetic Algorithm-Based Phishing Email Detection System** *Nov 2024*
  Tools: Python, Google Colab, Pandas, NumPy, Scikit-Learn, TF-IDF, Random Forest
  - Used a Genetic Algorithm to select key features from email text.
  - Trained a Random Forest classifier on TF-IDF processed email data.
  - Achieved 95.45% with strong precision and recall balance.
  - Evaluated performance using confusion matrix and metric comparison.
- **Deep Learning-Based Network Forensic Framework for APT Detection** *Nov 2024*
  Tools: Python, Google Colab, Pandas, NumPy, Scikit-Learn, TensorFlow/Keras
  - Developed a network forensic framework to detect Advanced Persistent Threat (APT) activity.
  - Trained an MLP deep neural network on the UNSW-NB15 dataset for anomaly identification.
  - Applied feature filtering and hyperparameter tuning to enhance detection accuracy.
  - Evaluated model performance using confusion matrix, ROC curve, and precision-recall metrics.

Skills

- **Cybersecurity & Network Defense:** Penetration Testing, SOC Monitoring, Threat Intelligence, Digital Forensics, Vulnerability Assessment, Incident Response, Risk Assessment, Threat Analysis, Network Security, Packet Analysis, Firewall/IDS Concepts, OWASP Top 10
- **Machine Learning for Security:** Anomaly Detection, K-Means, Random Forest, MLP/DNN, Model Evaluation, Hyperparameter Tuning
- **Programming & Development:** Python, C++, SQL, Bash, Flask, REST APIs, HTML/CSS/JavaScript
- **Security & Analysis Tools:** Burp Suite, PortSwigger Labs, Seed Labs, Wireshark, Nmap, Metasploit, Hashing & Encryption Libraries
- **Cloud, DevOps & Automation:** AWS, Terraform, Docker, GitHub Actions (CI/CD), Prometheus, Grafana
- **Soft Skills:** Project Coordination, Technical Documentation, Team Collaboration, Problem Solving

Awards

- **Dean's Honor Roll Award** — Achieved distinction GPA for five consecutive semesters with GPAs: 3.71 (Semester 3), 3.65 (Semester 4), 3.54 (Semester 5), 3.52 (Semester 6), 3.54 (Semester 7).

Leadership Experience

- **Member & Hackathon Head – ACM GIKI Chapter** *Sep 2023 – Present*
  Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (GIKI)
  - Organized and led technical competitions including Speed Programming, Game Development, and Hackathons.
  - Attracted and engaged 250+ participants annually, fostering innovation and community collaboration.
  - Managed full event lifecycle including planning, logistics, execution, and post-event reporting.
- **Head Member – Society for the Promotion of Higher Education in Pakistan (SOPHEP)** *Feb 2023 – Present*
  Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (GIKI)
  - Led the organization of major institutional events including GIMUN, GIKI Moot Cup, Career Fair, Educational Expo, and Industrial Open House.
  - Coordinated with 50+ industry leaders and academicians to deliver impactful networking and recruitment experiences.
  - Hosted events with 200+ participants annually from universities and organizations across Pakistan.

Additional Information

Languages: English (Fluent), Urdu (Fluent), Pashto (Native)

Interests: SOC Operations, Red Teaming, Football, Music, Traveling