**FATHIMA DIYA PATTANI SHAIK**

**Cybersecurity Graduate | Protecting Networks, Securing Systems, Driving Innovation**

E-Mail: fathimadiya481@gmail.com

**Summary**

Honours **Cybersecurity Graduate** with a strong foundation in network defense, vulnerability management, and threat detection. Certified in **CompTIA Security+** and **CySA+**, with hands-on experience in configuring firewalls, performing vulnerability scans, analyzing security logs, and conducting web application security testing. Skilled in tools such as **Kali Linux, OpenVAS, Burp Suite, Wireshark, and Splunk**, and knowledgeable in **Active Directory**, **SIEM**, and **incident response procedures**. Passionate about leveraging technical skills and analytical thinking to enhance system security and contribute effectively to an organization’s cybersecurity posture.

**Certifications:**

* **Certified in System Administrators by Microsoft**
* **Certified in CompTIA Security+**
* **Certified in CompTIA CySA+**

**Technical Skill:**

* **Networking & Security:** 
  + Protocols: TCP/IP, DNS, DHCP, VPN, VLAN, TLS/SSL, SNMP
  + Firewalls: Palo Alto (6 months hands-on), pfSense, Wazuh SIEM
  + Security Tools: Kali Linux, Burp Suite, Hydra, Volatility (memory forensics)
  + Frameworks: NIST, ISO 27001 compliance, disaster recovery planning
* **Systems & Cloud:** 
  + Active Directory, Group Policies, VMware/VirtualBox
  + AWS, Azure, Office 365 administration • Windows/Linux system administration
* **Development & Documentation:** 
  + Python, Java, JavaScript, and PowerShell scripting
  + Technical documentation (Word, Excel, Visio).

**Soft Skill:**

Strong communication, problem-solving, adaptability, attention to detail, time management, initiative, and teamwork skills

**Projects:**

* Network Vulnerability Assessment using OpenVAS
  + Performed comprehensive scans on a simulated enterprise network using OpenVAS to identify and categorize vulnerabilities.
  + Analyzed results, assessed risk levels, and proposed remediation strategies aligned with NIST security standards.
* Web Application Security Testing (OWASP Juice Shop)
  + Conducted penetration testing on the OWASP Juice Shop application to exploit and document OWASP Top 10 vulnerabilities such as XSS, SQL Injection, and Broken Authentication.
  + Provided mitigation recommendations and implemented secure coding practices to strengthen application security.
* Log Analysis and Threat Detection using Splunk
  + Configured Splunk to collect and analyze logs from simulated network devices and systems.
  + Created dashboards and alerts to detect suspicious activity, brute-force attempts, and unauthorized access patterns.
* File Integrity Monitoring using Python
  + Developed a Python-based File Integrity Checker that uses SHA-256 hashing to detect unauthorized file changes.
  + Automated alerts for integrity violations to improve data protection and early threat detection.
* Active Directory Security Lab
  + Built a Windows Server-based Active Directory environment for centralized user and policy management.
  + Implemented Group Policies, password rules, and access control measures following least privilege principles.
* Honeypot Deployment for Threat Monitoring
  + Deployed a Cowrie honeypot on a virtual network to collect and analyze attacker behavior and intrusion attempts.
  + Logged malicious IPs, command patterns, and payloads for security intelligence and incident response improvement.