Muhammad Saim Ch

Cybersecurity Student | SOC Analyst Aspirant

Saimc727@gmail.com
+92 315 755 0551
linkedin.com/in/muhammad-saim-ch/
github.com/muhammad-saim-ch
muhammad-saim-ch.me
Islamabad, Pakistan

SUMMARY

SOC-focused cybersecurity student with hands-on experience building IDS rules (Snort), analyzing network traffic (Wireshark), and developing automated vulnerability scanning/reporting tools using Python and Flask. Seeking a SOC Analyst internship to apply threat detection, log analysis, and incident response skills in real-world environments.

PROJECTS

Real-Time SOC Monitoring Dashboard ***Flask · Wazuh · Splunk · Snort · Python · Chart.js · Wireshark***

- Built a Flask-based SOC dashboard integrating Wazuh, Splunk, and Snort for real-time threat detection, log correlation, and automated incident reporting, simulating and detecting 10+ attack scenarios.

IDS / IPS Deployment & Threat Simulation ***Snort · Suricata · Zeek · Wazuh · Wireshark · Kali Linux***

- Deployed Snort, Suricata, Zeek, and Wazuh to simulate and detect brute-force, port scanning, and SQL injection attacks while improving alert accuracy through rule tuning.

Automated Vulnerability Scanner + Exploit Reporter ***Python · OpenVAS/Nessus · Metasploit · SQLmap · Flask · Chart.js***

- Developed a Python-based vulnerability assessment tool integrating OpenVAS/Nessus outputs with automated CVSS-based reporting and exploit validation workflows.

VPN Implementation ***OpenVPN · Linux CLI · PKI · Wireshark***

- Configured a secure OpenVPN lab environment with PKI authentication and analysed encrypted traffic using Wireshark to study secure remote communication.

AU Campus Navigation — Dijkstra's Algorithm ***C++, Data Structures***

- Modeled AU campus as a weighted graph; Dijkstra's algorithm finds shortest path across 20+ nodes in c++..

EDUCATION

BS Cybersecurity ***2024 – Present | 4th Semester***

Air University, Islamabad

SKILLS

SIEM / SOC	Wazuh · Splunk · Suricata · Zeek · Snort · OSSEC
Vulnerability Assess	Nessus · Nmap · Nikto · SQLMap · Burp Suite · Wireshark
Offensive	Metasploit · Kali Linux · VMware / VirtualBox
Languages	Python · Bash · C++ · Java
Web & Reporting	Flask, Chart.js, ReportLab, WordPress, SQL/SQLite.

CERTIFICATIONS & INTERESTS

- **NITSEP:** Penetration Testing Specialist
- **EC-Council:** SQL Injection
- **Cisco:** Ethical Hacking
- SOC / Blue Team Operations
- Threat Intelligence & Incident Response
- Network Security