Harris Sultan

SOC Analyst | Cybersecurity

harrissultan0@gmail.com 923156790054 Wah Cantt,Pakistan www.linkedin.com/in/harrissultan009

github.com/InventiveBear

Profile

Cybersecurity Analyst with hands-on experience in network traffic analysis, threat simulation, and secure application development. Strong foundation in SOC workflows, IDS/IPS concepts, and attack detection using Wireshark, Scapy, Burp Suite, and Kali Linux. Software engineering background with practical exposure to secure SDLC and OWASP principles.

Projects

Smurf Attack Demonstration (Python, Scapy)
- Simulated a Denial-of-Service (DoS) attack in a virtual lab using Python and Scapy on Kali Linux
- Monitored ICMP amplification and analyzed network traffic via Wireshark

Secure Web Application (Frontend)
- Built a secure landing page with HTML, CSS, and Bootstrap
- Implemented input validation to mitigate common web vulnerabilities

SOC 2 Security Evidence Analysis (SOC Operations Project), *REDTECHSOFT360*
- Analyzed organizational security evidence to assess SOC 2 Type I readiness.
- Reviewed risk assessments, scan results, and backup documentation to validate controls.
- Mapped controls to evidence to identify gaps and remediation priorities.
- Delivered concise security findings and recommendations aligned with SOC best practices.

Education

Masters in Information Security, *Riphah International University* 01/2019 – 07/2021
- Relevant Coursework: Cybersecurity, Linux, Data Analysis, Network Security, Python

SOFTWARE ENGINEERING, *COMSATS Institute, Wah Campus* 02/2014 – 01/2018
Relevant Coursework: SDLC, Web Development, Database Management

Skills & Tools

Security & Networking
- Wireshark, Burp Suite, Scapy, Kali Linux
- TCP/IP, IDS/IPS concepts, Traffic Analysis

Scripting & Development
- Python, Bash
- PHP, SQL, C#

Platforms
- Linux, Git, VMware

Experience

SOC Analyst, *REDTECHSOFT360* 01/2026 – Present
- Analyzed organizational security evidence to assess SOC 2 control effectiveness and audit readiness.
- Validated risk, vulnerability, backup, and access control evidence; identified control gaps.
- Delivered prioritized remediation recommendations aligned with SOC best practices.

Software Developer, *NRTC (National Radio & Telecommunication Corporation)* 02/2019 – 12/2019
- Assisted in developing and securing a web-based employee appraisal system
- Participated in application testing and design review, gaining insights into secure SDLC practices

Web Developer, *Sir Syed Society of School and Colleges* 04/2023 – 07/2023
- Enhanced PHP/CodeIgniter web apps with secure database handling in MySQL
- Followed OWASP secure coding principles

Courses & Learning

Web Security Academy Learning Paths, *Portswigger academy* present
- Hands-on labs focused on web vulnerabilities, request manipulation, and attack/defense techniques

Codeinplaces, *Stanford university* 04/2026 – 05/2026
Foundation in Python programming, problem-solving, control flow, functions, graphics, lists, and dictionaries while building practical programming projects