Muhammad Bassam Khan

Cybersecurity Engineer with a passion for Machine Learning and Pentesting

☎ +92 3399114411
@ bassam.exe@gmail.com
Medium
Github: github.com/MasterChief220
LinkedIn: in/mbassamkhan/
Website

Skills

Defensive Security & SOC Engineering

SIEM, EDR, Malware Analysis, Packet Analysis, Vulnerability Assessment, NDR

Offensive Security & Red Teaming

Nmap, Wireshark, Burp Suite, Metasploit, OWASP ZAP, Hydra, Mimikatz, Hashcat

Programming

Web Scraping, Web Automation, Python, Bash, MySQL, C++

Certifications

Certified SOC Analyst
EC-Council
May 2025

SOC Level 1
TryHackMe
Jan 2025 (87 hours)

Junior Penetration Testing Pathway
TryHackMe
Oct 2023 (91 hours)

Google Cybersecurity Certificate
Coursera- Google
Sept 2023 (126 hours)

Supervised Machine Learning: Regression and Classification
Coursera- Deeplearning AI
Jun 2023 (32 hours)

Additional Certifications

Developing Front-End Apps with React
Coursera- IBM
Oct 2023 (14 hours)

Python, Bash and SQL Essentials for Data Engineering
Coursera- Duke University
Oct 2023 (183 hours)

Education

NUST- Islamabad — **September 2020- June 2024**
Mechatronics — Engineering

Nixor College- Karachi — **August 2018- June 2020**
Pre-Engineering — Alevels

Experience

National Radio and Telecommunications Corporation — **September 2024- Present**
Assistant Executive Engineer Cybersecurity — Islamabad, Pakistan
Website

- Designed and deployed a sectoral Security Operations Center (SOC) model to aggregate alerts from 5+ sub-organizational SOCs into a central NRTC dashboard, enabling escalation to the national-level SOC (directorate).
- Built and deployed a SIEM proof-of-concept using the ELK Stack (Elasticsearch, Logstash, Kibana) on internal servers; configured Winlogbeat, Auditbeat, and syslog pipelines to ingest and visualize logs from 50+ endpoints and agentless network devices (routers, switches).
- Performed internal penetration testing and vulnerability assessments, uncovering flaws such as XSS and SQL injection using tools like Burp Suite, Nmap, and OWASP ZAP.

National Cybersecurity Emergency Response Team (via NRTC) — **December 2024- June 2025**
Pak Secretariat- Islamabad, Pakistan
SOC Analyst
Website

- Conducted malware analysis on 15+ samples using static (e.g., PEStudio, strings) and dynamic (e.g., any.run, hybrid-analysis) techniques to extract behavior patterns and command-and-control (C2) infrastructure.
- Led vulnerability assessments and penetration tests on 50+ critical government websites using Burp Suite, ZAP, Metasploit, Nessus, and Nmap, identifying RCEs, weak configurations, and outdated libraries.
- Deployed EDR and enforced GPO baselines on 20+ endpoints, reducing alert fatigue by 25%.
- Performed OSINT investigations on IOCs using passive DNS, WHOIS, Shodan, and threat intelligence feeds to support attribution and detection enhancement.

Fauji Foundation — **September 2023- October 2023**
Networking/Cybersecurity Intern — Rawalpindi

- Configured and simulated enterprise networks with 20+ routers and switches in Packet Tracer, implementing VLANs, trunking, and STP for optimized segmentation.
- Performed subnetting and network segmentation across simulated topologies, prioritizing cybersecurity principles in design.
- Analyzed 100+ packets and scanned 50+ hosts using Wireshark, Nmap, and Traceroute to identify vulnerabilities and reduce open ports exposure.

Projects

RapidScan Automation and Enhancement — **Jan 2025**
Github

- Enhanced the existing RapidScan vulnerability scanner by extending its capabilities to support batch scanning of multiple domains, adding a `` `--list` `` argument and modular execution logic.
- Simplified large-scale recon workflows in red teaming and CTF scenarios by integrating input file parsing, dynamic subprocess handling, and result logging.