





Muhammad Bassam Khan


Cybersecurity Engineer with a passion for Machine Learning and Pentesting

 +92 3101144100

 bassam.exe@gmail.com

 [Medium](#)

 Github: github.com/MasterChief220

 LinkedIn: [in/mbassamkhan/](https://in.linkedin.com/in/mbassamkhan/)

Skills

Programming

Pandas, Web Scraping, Numpy, Web Automation, Scikit, Python, Bash, MySQL, C++, Microcontroller Programming

Machine Learning

Regression, Q Learning, Classification, Tensorflow, OpenCV

Pentesting

Nmap, Wireshark, Burp Suite, Traceroute, Metasploit

Engineering

AutoCAD, LabVIEW, Matlab, Proteus, Rslogix

Certifications

SOC Level 1

TryHackMe

Google Cybersecurity Certificate

Coursera

Junior Penetration Testing Pathway

TryHackMe

Python, Bash and SQL Essentials for Data Engineering

Coursera

Developing Front-End Apps with React

Coursera

Introduction to Quantum Computing

Udemy

Reverse Engineering .NET for Beginners (Visual Basic)

Udemy

Supervised Machine Learning: Regression and Classification

Coursera

Ethical Hacking Essentials (EHE)

EC-Council

Introduction to Bash Shell Scripting

Coursera

IOSH-UK

Safecon

Education

NUST
Mechatronics

September 2020– June 2024
Engineering

Nixor College
Pre-Engineering

August 2018– June 2020
Alevels

Experience

NRTC
Assistant Executive Engineer Cybersecurity

September 2024– Present
Islamabad

- Manage and configure Security Information and Event Management (SIEM) tools to monitor and analyze security threats in real-time.
- Deploy and integrate Network Detection and Response (NDR) systems to detect anomalous activities and enhance network visibility.
- Implement Endpoint Detection and Response (EDR) solutions to provide advanced endpoint security, identifying and mitigating potential threats on end-user devices.
- Conduct vulnerability assessments and penetration testing on websites and servers as part of operations with NCERT (National Cybersecurity Emergency Response Team of Pakistan) to identify and remediate security weaknesses.
- Perform static and dynamic malware analysis to detect, dissect, and mitigate potential threats.
- Monitor, analyze, and respond to security incidents in real-time as a SOC Analyst, leveraging SIEM, EDR, and threat intelligence tools to enhance threat detection and response capabilities.

Fauji Foundation Head office
Networking/Cybersecurity Intern

September 2023– October
Rawalpindi

- Acquired an in-depth understanding of the OSI model and its seven layers.
- Designed and simulated networks using Packet Tracer, configuring over 20 switches and routers, implementing VLANs, trunking lines, and STP.
- Demonstrated expertise in subnetting, network segmentation, and prioritizing cybersecurity in network design.
- Proficiently utilized packet analysis tools such as Wireshark and network scanning tools like Nmap, Traceroute to identify and close open ports.

Projects

Computer Vision Car Counter
NUST Project

May 2023

 [Github](#)

- Detected cars in a video frame and counted them using Image Processing using a pre-trained Haar Cascade Classifier.
- Employed a pre-trained Haar Cascade Classifier to accurately detect cars in video frames, achieving a detection accuracy of over 90%.
- Processed video footage at an average rate of 30 frames per second, ensuring real-time detection and counting.

SIEM Deployment

Elasticsearch and Syslog

- Designed and implemented a self-hosted Elasticsearch setup on a VM, configuring Winlogbeat and Auditbeat for log collection and analysis.
- Configured Logstash to receive syslogs, demonstrating a proof of concept (PoC) for collecting logs from agentless devices like switches and servers.