

Malik Touseef Husnain

 touseef25@outlook.com |  +92 300 5505252

 cyberseef.com |  linkedin.com/in/cyberseef

Professional Summary

Cybersecurity specialist with 2+ years of remote freelance experience in threat hunting, penetration testing, and digital forensics. Strong foundation in malware analysis, DFIR tools, and security frameworks. Delivered client projects across platforms like SEED Labs and Snort-based IDS systems. Passionate about securing modern infrastructure with hands-on knowledge of network security, cloud platforms (AWS), and machine learning applications. Actively seeking remote opportunities in blue/red teams, SOC, or cybersecurity research.

Professional Experience

GRC & Penetration Testing Intern

Pakistan Cyber Emergency Response Team — July 2025 – Aug 2025

- Studying and working on ISO standards.
- Working on other supervised GRC related responsibilities.
- Additionally, volunteered for Software Security Testing.

Freelancer – Cybersecurity Consultant

Fiverr (Remote) — Nov 2021 – Nov 2023

- Delivered over 30+ client projects in malware analysis, vulnerability assessment, and digital forensics
- Built a smart home honeypot using Snort and anomaly detection ML model
- Mentored students in SEED Labs, DVWA, and OWASP challenges
- Designed and deployed lab environments using virtualized infrastructure

Cybersecurity Mentor

STEM Wizards Academia (Remote) — Dec 2022 – Apr 2023

- Guided participants in Girls Technovation Program to develop secure mobile/web apps
- Supervised development of an AI-powered secure messaging app with malicious link detection
- Conducted code reviews and recommended secure coding practices

Intern – Cyber Threat Hunter

ThincsCorp (Remote) — Jul 2022 – Oct 2022

- Conducted real-world threat hunting using IOCs and TTPs aligned with MITRE ATT&CK
- Supported development of threat intelligence reports and enriched IOC datasets
- Practiced log correlation and threat emulation across lab environments

Key Projects

Final Year Project

EagleAI – AI-Based Network Intrusion Detection & Prevention System (IDPS)

- Developed a DDoS detection system using supervised ML models on CIC DDoS 2019 dataset
- Created pipeline for traffic collection, preprocessing, and anomaly scoring
- Technologies: Python, AutoML, TensorFlow, InfluxDB, Flask, Wireshark

Smart Home Honeypot IDS

- Created an ML-based intrusion detection honeypot for IoT/Smart Home environment
- Used Snort and custom Python scripts to emulate intrusion events
- Delivered full project with documentation and alert dashboards

Certifications

- Certified Red Team Operations Management (CRTOM) – Red Team Leaders
- Certified Cybersecurity Educator Professional (CCEP) - Red Team Leaders
- Blue Team Junior Analyst (BTJA) - Security Blue Team
- Certified Cloud Security Practitioner (CCSP-AWS) - SecOps Group
- Certified Network Security Practitioner (CNSP) - SecOps Group
- Certified AppSec Practitioner (CAP) - SecOps Group
- Foundation Threat Intelligence Analyst (FLTA) - arcX
- Maximizing DFIR Results with YARA & Sigma – Belkasoft
- Polaris's Human Trafficking 101 Training - Polaris
- Belkasoft X Mobile Forensics - Belkasoft

Technical Skills

- Tools: Wireshark, Belkasoft X, Snort, Splunk, ELK, YARA, Sigma, Autopsy, FTK Imager
- Languages: Python, Bash, JavaScript
- Security Domains: DFIR, Threat Hunting, AppSec, CloudSec, Pen Testing, SIEM
- Cloud: AWS (IAM, CloudTrail, EC2), Heroku
- Frameworks: MITRE ATT&CK, OWASP Top 10, NIST

Education

FAST NUCES – National University of Computer & Emerging Sciences

Bachelor's in Cyber Security — 2019 – 2025

Final Year Project: EagleAI – AI-Based IDPS for DDoS Detection

Cadet College Hasanabdal

Intermediate (Pre-Engineering) — 2017 – 2019

Matriculation (Biology) — 2015 – 2017

Remote Readiness

- 2+ years experience working with global clients
- Fluent in English (written & spoken), experienced with remote collaboration
- Comfortable with tools like Zoom, Slack, Trello, Jira, Notion, GitHub