Muhammad Javed Waqas

[Your Email] [Your Phone Number] in/[LinkedIn Profile Link]

SUMMARY

Aspiring Cybersecurity Professional and SOC Analyst with a strong foundation in network security, log analysis, and penetration testing. Active security researcher currently ranked in the **Top 15% globally on TryHackMe**, demonstrating rapid progression from the Top 50% to the Top 15% within 15 days through consistent hands-on lab completion on TryHackMe with a proven track record of solving complex labs involving Active Directory, Linux internals, and PowerShell. Currently transitioning from foundational learning to professional application, with a focus on building automated detection systems and preparing for the OSCP.

EXPERIENCE

Active Security Researcher

TryHackMe

- Rank: Top 15% (Global) | Points: 4000+ (Current Milestone)
- Completed Learning Paths: Cyber Security 101, Linux Fundamentals, Active Directory Basics.
- Consistently solving "Challenge" rooms to master manual exploitation and defense techniques.

PROJECT

Web Authentication Project

PHP & Render

- Designed and deployed a secure web login system, currently migrating to a hardened WordPress environment.
- Conducted vulnerability assessments using Burp Suite to identify and remediate authentication flaws.
- Managed cloud deployment and environment variables via Render.

Hybrid SOC Detection Lab

Splunk & Suricata

- Engineered a virtualized security environment to correlate network IDS alerts with host-based logs.
- Developed custom SPL queries to identify and alert on high-frequency request patterns and brute-force attempts.
- Configured automated reporting for "First Time Seen" IP addresses to improve incident response times.

CERTIFICATIONS

BCP/DRP Frameworks

April 2026

- Gaining expertise in maintaining organizational resilience and recovery during security incidents.
- Applied for isc2 certified in cyber security exam.

SKILLS

Compliance & Strategy: Business Continuity Planning (BCP), Disaster Recovery Planning (DRP)

Networking: TCP/IP, DNS, HTTP/S, SSH, Packet Analysis

Operating Systems: Linux (Advanced CLI: awk, grep, chmod), Windows & PowerShell

Security Tools: Nmap, Metasploit, Burp , Wireshark

SIEM & Monitoring: Splunk Enterprise (Alerting, Dashboards, SPL)