Shahzeb Ali

Cybersecurity Analyst

Address: Madinat Zayed, Abu Dhabi, UAE
Phone: +971586112232
Email: ishahzebali@aol.com
https://www.linkedin.com/in/ishahzebali

Summary

Entry-level SOC Analyst with a Bachelor's in Computer Science and certifications in SOC L1 and Pre-Security. Skilled in incident triage, log analysis, and penetration testing tools like Nmap and Metasploit to enhance threat detection via SIEM and EDR. Eager to apply purple team expertise in a dynamic security operations environment to mitigate risks and support organizational resilience.

Skills & tools

Defensive Operations (Blue Team): Incident Triage, Log Analysis (SIEM), Phishing Analysis, Malware Analysis, Threat Intelligence, IOC Extraction.
Offensive Operations (Red Team): Vulnerability Scanning, Network Enumeration, Web Application Exploitation (OWASP Top 10), Privilege Escalation.
Networking & Systems: TCP/IP, OSI Model, DNS, HTTP/S, Linux CLI, Windows Internals, Active Directory basics.
Soft Skills: Analytical Thinking and Problem-Solving, Attention to Detail, Team Collaboration and Communication
Tools:

- **Defensive:** Splunk, ELK Stack,MS Sentinel, Wireshark, TheHive, Cortex.
- **Offensive:** Nmap, Burp Suite, Metasploit, Hydra, Gobuster.
- **Frameworks:** MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain.

Projects

Independent Security Researcher | *YesWeHack Nov 2025 – Present*

- Conducted black-box security testing on web applications, focusing on OWASP Top 10 vulnerabilities like Broken Access Control and IDOR.
- Successfully uncovered and reported a logic vulnerability in a major music streaming platform (Deezer), resulting in a patch and bounty reward.

- Analyzed HTTP traffic using Burp Suite to identify discrepancies between client-side controls and server-side validation.

Mastercard Cybersecurity virtual experience program on Forage - December 2025

- Completed a job simulation where I served as an analyst on Mastercard's Security Awareness Team
- Helped identify and report security threats such as phishing
- Analyzed and identified which areas of the business needed more robust security training and implemented training courses and procedures for those teams

Deloitte Australia Cyber Job Simulation on Forage - December 2025

- Completed a job simulation involving reading web activity logs
- Supported a client in a cyber security breach
- Answered questions to identify suspicious user activity

Enterprise Phishing & Data Exfiltration Simulation on - TryHackMe - December 2025

- Conducted a full-lifecycle investigation of a compromised endpoint, reconstructing the Cyber Kill Chain from initial phishing access to data exfiltration.
- Analyzed Sysmon logs to detect "Living off the Land" (LotL) tactics, distinguishing malicious use of Robocopy(for data staging) and PowerShell from benign system noise.
- Identified advanced post-exploitation activities, including network reconnaissance via PowerView and stealthy data theft via DNS Tunneling (decoding Base64 payloads).
- Tools: Sysmon, Log Analysis, Phishing Forensics, MITRE ATT&CK Mapping.

Certifications

- SOC L1 - TryHackMe.
- CyberSecurity 101 - TryHackMe.
- Pre-Security - TryHackMe.
- Python - Codedex.
- Bash Scripting - CodeAcademy.

Education

Bachelor's degree in Computer Science

Lahore Garrison University - Lahore, Punjab, Pakistan

2020 - 2025