Rehan Ahmad

+92-313-4771723 | rehanathome78@gmail.com | Lahore, Pakistan | GitHub

PROFESSIONAL SUMMARY

Cybersecurity Analyst with a strong foundation in Incident Response and Threat Detection. Expertise in Log Analysis (SIEM/Splunk), Packet Analysis, and Security Automation (Python). Dedicated to defending organizational assets using a systematic approach guided by the NIST CSF and CIA Triad.

SKILLS & CREDENTIALS

CERTIFICATIONS: Google Cybersecurity Professional Certificate (Completed), CompTIA CySA+ (Planned), Generative AI (Dec 2023), Full Stack Web Development (May 2022)

TECHNICAL SKILLS:

- **Tools:** SIEM (Splunk), Packet Analysis (Wireshark, tcpdump), Log Analysis (SQL), Incident Response, Nmap, Firewall Rules, MFA Implementation
- **Frameworks:** NIST CSF, CIA Triad, OWASP Top 10, MITRE ATT&CK
- **Scripting & OS:** Python (Automation), Linux CLI, PHP, JavaScript, Git
- **Networking:** TCP/IP, DNS, VPN, Ingress/Egress Filtering, Access Control (MAC, DAC, RBAC)

PROJECTS

Security Automation Scripting: Python Log Parsing

- Automated log parsing and filtration by developing a Python script for IoC detection
- Script is estimated to reduce manual event triage time by 40%, increasing SOC efficiency

Internal Security Audit: NIST CSF Compliance

- Conducted a comprehensive NIST CSF-based risk and compliance audit in a simulated environment
- Identified five critical security posture gaps and recommended remediation, improving theoretical security baseline by 25%

Brute Force Attack Case Study: HTTP & DNS Log Analysis

- Analyzed logs using SQL filters and INNER JOINs to trace suspicious login activities
- Minimized potential attacker dwell time by successfully identifying multiple brute-force login attempts and proposing remediation steps

EXPERIENCE

WordPress Developer | The Rehan Dev & Fiverr, Remote **|** Jan 2022 - Present

- Maintained system integrity via Git-based version control for rapid rollback, improving deployment reliability and recovery time (RTO) by 30%.
- Ensured high system availability by executing continuous security updates and vulnerability patching, preventing unscheduled downtime (a core security goal)

WordPress Developer | Career Adviser & Hassan Associates, Lahore | Aug 2020 – Jan 2023

- Resolved critical technical and operational issues by coordinating with leadership, demonstrating clear stakeholder communication during system triage
- Managed CMS to ensure stability and reduced attack surface by implementing basic security and access controls

EDUCATION

BBIT, Management Science | Virtual University of Pakistan (Aug 2024 – Aug 2028)

Aspire Leaders Program | Aspire Institute (Jan 2024 – Apr 2024)