Rehan Ahmad

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

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in threat detection, incident response, vulnerability assessment, and security hardening through the Google Cybersecurity Certificate. Skilled in SIEM (Splunk), packet analysis (Wireshark, tcpdump), firewall configuration, and access control models (MAC, DAC, RBAC). Previously worked in full-stack development (PHP, React, Node.js, WordPress, Dreamweaver), creating websites with a focus on security best practices, including OWASP guidelines, access control, and data protection. Proficient in applying NIST CSF and CIA Triad principles to safeguard digital assets and ensure resilience.

EDUCATION

BBIT, Management Science **Aug 2024 - Aug 2028**
Virtual University of Pakistan

Aspire Leaders Program **Jan 2024 - Apr 2024**
Aspire Institute (co-founded by Harvard Business School Professors)

EXPERIENCE

WordPress Developer Intern **Nov 2022 - Jan 2023**
Career Adviser, Remote

- Designed and managed website content updates and enhancements
- Coordinated directly with CTO and CEO to implement feature requests
- Supported website stability and uptime using CMS tools and basic security checks

WordPress Developer **Aug 2020 - Aug 2021**
Hassan Associates, Lahore

- Developed and maintained WordPress website with strong emphasis on security best practices
- Collaborated with stakeholders to define, design, and deploy responsive, SEO-optimized website
- Applied version control using Git to manage site updates and plugin integration
- Troubleshoot cross-browser compatibility issues and optimized site performance

CERTIFICATIONS

- **CompTIA CySA+**, CompTIA, (**Planned)** - Target Completion: Nov 2025
- **Google Cybersecurity Professional Certificate**, Google - Dec 2024
- **Generative AI for Everyone**, DeepLearning.AI - Dec 2023
- **Full Stack Web Development**, Ideoversity - May 2022
- **2024 Aspire Leaders Program**, Aspire Institute – April 2024

SKILLS

- **Security:** Incident Response, Threat Detection, Vulnerability Assessment, Security Hardening, SIEM (Splunk), Packet Analysis (Wireshark, tcpdump), Firewall Rules, Ingress/Egress Filtering, MFA Implementation, Log Analysis, Access Control (MAC, DAC, RBAC)

- **Frameworks & Standards:** NIST Cybersecurity Framework (CSF), CIA Triad, OWASP Top 10
- **Networking:** TCP/IP, DNS, HTTP/HTTPS, LAN/WAN, VPN, ICMP
- **Programming & Scripting:** PHP, JavaScript, React, Node.js, Python, TypeScript, SQL
- **Web & CMS:** WordPress (Custom Themes, Plugins, REST API), Dreamweaver
- **OS & Tools:** Linux CLI, chmod, Nmap, Git

PROJECTS

Internal Security Audit
Botium Toys
- Conducted an NIST CSF-based audit for a fictional company, including risk assessment, compliance checklist, and security self-assessment
- Identified gaps in security posture and recommended improvements aligned with industry standards

SYN Flood Case Study
Network Attack Analysis
- Investigated a SYN flood DoS attack using Wireshark
- Differentiated between normal and malicious TCP traffic, prepared a professional incident report with mitigation strategies

Brute Force Attack Case Study
HTTP & DNS Log Analysis
- Analyzed tcpdump logs to trace DNS and HTTP traffic patterns in a simulated web server compromise
- Identified brute-force login attempts, documented findings, and proposed remediation steps

Analysis of Network Hardening
- Examined a real-world breach scenario at a social media company
- Found vulnerabilities like shared passwords and weak firewall rules, proposed targeted solutions including MFA and stricter firewall enforcement

Linux File Permissions Project
Secure File & Directory Access
- Managed Linux file permissions using `ls -la` and `chmod` to apply the principle of least privilege
- Secured sensitive files, adjusted directory access, and removed unnecessary write permissions

Apply Filters to SQL Queries
Cybersecurity Data Investigation
- Investigated suspicious login activities using SQL filters (`AND`, `OR`, `NOT`, `LIKE`) and `INNER JOIN`
- Correlated user activity with employee records to detect anomalies and support incident investigations