RAZA **AZEEM**

Zaida, Swabi 23540 | +92-335-7735900 raza_azeem@outlook.com

Websites, Portfolios, Profiles

- www.linkedin.com/in/razaazeem
- https://razaazem.github.io/Portfolio/

Professional Summary:

Experienced IT Services Engineer with a strong record of delivering exceptional technical support and efficiently managing IT infrastructure. Seeking an opportunity as an Information Security Analyst, VAPT Analyst, SOC Analyst, to leverage my extensive expertise and further develop skills in the dynamic field of information security. Committed to ensuring the confidentiality, integrity, and availability of critical data and systems, dedicated to staying updated on emerging technologies and industry best practices to effectively mitigate risks and safeguard organizational assets.

Educations:

Bahria University (2023)
MS Information Security
Relevant Courses: Information Security Management, Digital Forensics, Cyber Security, Penetration testing, Cloud computing security.

Abbottabad University (AUST) (2019)
BS Computer Science
Relevant Course: Database Management System, Compiler Construction, Computer and Network Communication, Management Information System.

Awards & Certifications:

- **Practical Ethical Hacking** - TCM Security
- **IBM Cybersecurity Analyst** - IBM
- **Diploma Cyber Security** - eLearning
- **CompTIA CSA+** - InfoSec4TC
- **(ISC)^2 (CC)** - ISC2Official (ISC)^2
- **SOC Foundation Analyst** - SIEM XPERT
- **Red Hat Enterprise Linux** - Red Hat
- **ISO/IEC 27001:2022** - Skill Front
- **(CCNA) Security** - CyberTech Academy

Skills & Tools:
Vulnerability Assessment and Penetration Testing, Malware Analysis, Security Controls, Security Information and Event Management (SIEM), Microsoft Azure, Nessus Professional, Nikto, Aucnetix, Burp Suite, Metasploit, Beef, VMWare-Esxi, Wireshark, Nmap, mobsf, CyberArk.

Professional Experiences:

Pakistan Tobacco Company / HRSPL IT Service Engineer (2022 -- Present)

Key Responsibilities:

- Conquer diverse IT challenges: Provide expert technical support for all users, tackling issues related to security, hardware, software, network connectivity, and OT/ICS.
- Master incident resolution: Resolve incidents logged on ServiceNow, adhering to established procedures and SLAs. Utilize CyberArk for secure remote support and manage privileged account access controls.
- Safeguard OT/ICS systems: Proactively monitor performance and security, identifying and addressing potential issues.

- Collaborate with OT/ICS personnel to optimize functionality.
- Conduct thorough yearly and quarterly audits to ensure compliance.
- Team up with SIEM Security: Investigate compromised systems in collaboration with SIEM security, contributing to a robust security posture.

Emigrates **Help Desk Engineer** **(2019 -- 2020)**

Key Responsibilities:

- Managed and maintained system infrastructure, including servers, storage, and networking devices.
- Installed and configured software and hardware, including operating systems, security software, and applications.
- Troubleshooted and resolved system problems, such as performance issues, network outages, and hardware failures.
- Performed system backups and restores to ensure data protection.
- Monitored system performance and made necessary adjustments to maintain optimal performance.
- Provided technical support to users on system issues, such as account access issues and software problems.

Sense learner **Cyber Security & EH Internship** **(Aug,2023 -- Oct ,2023)**

Key Responsibility:

- Established foundational ethical hacking knowledge, complemented by hands-on experience in configuring a virtual environment using VMware and Kali Linux.
- Conducted OSINT on different Websites, produced a detailed and actionable report using information gathering tools.
- Gained knowledge about Vulnerability Assessment and Penetration Testing (VAPT), leveraging tools like Nessus, Metasploit and Poster for comprehensive scanning, coupled with practical application in solving labs on TryHackMe. Additionally, deepened comprehension of CVE, CWE, and NVD and sans top 25 Security Vulnerabilities.
- Researched and Analyzed Phishing Exploitation Techniques, Exploration and Mitigation Strategies and crafted a comprehensive report.
- Completed OWASP TOP 10 lab on TryHackMe, showcasing skills in identifying and mitigating web vulnerabilities. Conducted research on diverse web application attacks.