Zahid Hasan | [zh61966@gmail.com](mailto:zh61966@gmail.com) | +1-647-999-8976 | linkedin.com/in/zahid-hasan-a2155121a/

Conduct Penetration Tests: Perform thorough and methodical penetration testing on web applications, network infrastructures, and other systems to identify security vulnerabilities. Vulnerability Assessment: Assess and analyze security weaknesses and provide actionable recommendations to mitigate risks and improve overall security posture. Report Findings: Document and communicate findings clearly and effectively to both technical and non-technical stakeholders. Prepare comprehensive reports with recommendations for remediation. Develop and Execute Test Plans: Design and execute detailed test plans Stay Current: Keep up-to-date with the latest security trends, vulnerabilities, and tools to ensure testing methodologies are current and effective. Collaborate with Teams: Work closely with IT and development teams to understand system architectures, provide guidance on security best practices, and support the implementation of security improvements. Perform Risk Assessments: Evaluate and assess potential security risks related to new and existing systems and technologies. Compliance: Ensure that penetration testing practices comply with relevant regulations, standards, and organizational policies. Requirements: University degree Information security certification / accreditation an asset 7+ years of relevant experience Technical Skills: Proficiency in penetration testing tools such as Metasploit, Burp Suite, Nmap, and Kali. Knowledge of common web application vulnerabilities (e.g., OWASP Top Ten) and network security principles. Analytical Skills: Strong analytical and problem-solving abilities with attention to detail. Communication: Excellent verbal and written communication skills, with the ability to convey complex technical concepts to non-technical stakeholders. Ethical Standards: Demonstrated understanding of ethical hacking principles and a commitment to maintaining high ethical standards. Preferred Qualifications: Experience with penetration testing in cloud environments (e.g., AWS, Azure) and PCI testing. Familiarity with security standards and frameworks Certifications: Relevant certifications such as Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), or GIAC Penetration Tester (GPEN) are highly desirable

**Objective :** Detail-oriented and proactive Cyber Security Analyst with a strong foundation in identifying vulnerabilities and mitigating risks to protect sensitive data. Seeking to leverage my expertise in threat analysis, incident response, and security best practices at Raise. Committed to enhancing the security posture of financial services through continuous monitoring, strategic threat assessment, and collaboration with cross-functional teams to safeguard customer trust and confidentiality.

**Education**

* Diploma in Cybersecurity | Toronto School of Management | January 2022 – January 2023
* B.Tech | Computer Programming | Niagara College | May 2023 – Present

**Languages :** English, French (Amateur – learning ), Arabic, Bangla, Hindi, Urdu

**Projects:**

* Game Arcade App Development | PowerApps (2022) | [Game Arcade Project](https://www.linkedin.com/posts/zahid-hasan-a2155121a_gamearcade-gaming-tech-activity-7223148395090100224-iHol?utm_source=share&utm_medium=member_desktop)
* Concert Management - https://github.com/zahidhasan61966/new\_concert.git
* Figma UI/UX design

**Employment Experience**

**CyberSecurity | Capstone Project |** Toronto School of Management | 2022 – 2023

* Assisted in lab setups for Windows and Linux environments, supporting students in troubleshooting and configuration.
* Installed and configured various servers, including Windows Server roles (AD DS, DNS, DHCP) and Linux tools for cybersecurity training.
* Educated students on security protocols, vulnerability assessments, and penetration testing using tools like Wireshark, Nmap, and OpenSSL.

**Software Developer| Co-Op |** Niagara College Toronto | Ontario, Canada | 2023 - 2024

* Assisted in developing communications materials, enhancing accessibility with document conversion tools.
* Supported SharePoint administration, improving document collaboration and management processes.

**IT Technical Support Specialist |** Wadi Maramer Trading Group | Kingdom of Saudi Arabia | January 2018 – January 2020

* Led the deployment, configuration, and troubleshooting of network and server systems, enhancing operational efficiency.
* Maintained and documented software and hardware installations, ensuring compliance with industry standards.
* Oversaw IT equipment inventory and managed the lifecycle of assets, optimizing asset tracking and management processes.

**Certifications**

* Penetration Testing - CodeRed
* Cisco Cyber Security Essentials
* Multi-Cloud Network Associate Engineer - Aviatrix
* CISO – Network Security
* Nvidia: Fundamentals of Accelerated Computing
* The Odin Project

**Profile**

* Analytical problem-solver with a proactive approach to identifying and troubleshooting technical issues.
* Skilled in clear, effective communication with technical and non-technical audiences.
* Strong ethical standards, dedicated to confidentiality, and committed to upholding security best practices.
* Quick learner with a passion for emerging web technologies and a drive to continually develop new skills.

**Technical Skills**

* Penetration Testing: Experienced with tools like Wireshark, Nmap, and vulnerability scanning.
* Network Security: Knowledge of LAN/WAN, TCP/IP, DNS, DHCP, and security protocols (HTTPS, SSL/TLS).
* Operating Systems Security: Proficient in configuring and securing Windows Server environments (2012/2016/2019/2022) and various Linux distributions (Ubuntu, Kali, Parrot).
* Incident Response: Familiar with IDS/IPS, NIDS, and NIPS for threat detection and response.
* Database Security: Understanding of SQL and NoSQL database management and security practices.
* Risk Management: Knowledge of security policies and compliance frameworks.
* Development Security: Awareness of secure coding practices in web development (HTML5, CSS3, JavaScript, Node.js, PHP).
* Backup and Recovery Solutions: Experience with data backup strategies and disaster recovery planning.
* Technical Documentation: Ability to create and maintain security-related documentation and reports. project Experience

**References:** available upon request.