Sabeeruddin Shaik

P: (838) 202-2770 LinkedIn **E:** sabeeruddinshaik55@gmail.com

Risk Assessment | Network Vulnerability Scan | Encryption | Traffic Analysis | Web Application | Penetration Testing | Ethical Hacking | Phishing Analysis and Response | Malware Analysis | Intrusion Detection & Prevention

Summary:

- Highly skilled and detail-oriented Master of Digital Forensic and Cybersecurity graduating student with a keen interest in Cyber Security Analyst, Network Security Engineer, IT/ Cyber Security Consultant, SOC Analyst, or Security Incident Responder.
- Experienced in planning, managing, and upgrading security measures for data, systems, and networks.
- Strong troubleshooting abilities for security and network issues. Knowledgeable in change management, vulnerability testing, and risk assessments. Proven track record in implementing security controls to protect data and infrastructure.
- Proficient in researching technical issues and analyzing log files. Collaborative team player focused on enhancing information security.
- Monitoring network performance to determine adjustments and conferring with network users about solving problems.
- Experienced in designing security policies and supporting Windows servers. Proficient in installing and operating firewalls and encryption programs. Strong administration and maintenance skills for computer networks.
- Attending meetings with the cybersecurity team to discuss potential security threats and identify opportunities to enhance information security measures for users on the portal.

Education:

- **University at Albany - State University of New York, Albany, NY | GPA: 3.34** **Aug 2023**
- Master in Digital Forensics and Cybersecurity
- **Relevant Coursework:** Cybersecurity threats and controls, Network Security, Data Protection, Firewall and Intrusion Detection, Risk Management, Malware Analysis, Cyber Security Laws, Vulnerability Management, Digital Forensics, Incident Response, and Managing a Cyber Security Operations Center
- **Jawaharlal Nehru Technological University, India:** Bachelor in Civil Engineering **Aug 2021**

Certifications:

- **CompTIA Security+:** Maintain & Secure corporate IT system & network in accordance with industry standards & best practices.(July 2023)
- **Certified in Cyber Security (ISC2):** Gained comprehensive knowledge and practical expertise in the field of cybersecurity, enabling to effectively tackle real-world cyber threats and protect organizations from sophisticated attacks(Aug 2023).
- **Ethical Hacking & Pentesting:** Expertized in ethical hacking, penetration testing, vulnerability assessment, and risk analysis (Dec 2022)
- **AWS Certified Cloud Practitioner:** Proficient in utilizing AWS features such as IAM, EC2, Cloud Front, S3, SQS, and SNS.

Technical Skills:

- **Programming Languages:** Python, Java, SQL, Shell Scripting **| Analytical:** MS Excel
- **Networking Firewalls:** OSI Model, TCP/IP, Firewalls / IPS/IDS, Networking Protocols, Meraki Firewalls, Cisco Firewalls
- **GCP:** Docker, Kubernetes, Terraform, Compute Engine, App Engine, Cloud VPN, Cloud Function, Load Balancing Configuration
- **Networking:** LAN/WAN Technologies (TCP/IP, DHCP, DNS, NAT, ARP, UDP), Bluetooth, CDN, Active Directory, LDAP, TACACS
- **Cyber Security Tools:** Wireshark, Metasploit, VMware, Snort, Nessus, Nmap, Splunk, IBM QRadar, Burp Suite, cryptography (OpenSSL), Brute force (John), Kali Linux, CAINE, Qualys, Cisco Packet Tracer, Autopsy, MS Visio, Idesigner, OpenVas, Aircrack-ng, Nagios
- **Core Competencies:** Project Management, Relationship Building, Security Risk Assessment, Consulting, Cybersecurity, IT Support & Management, Root Cause Analysis, Systems Administration, Cloud Computing, Agile Approach, Collaboration
- **Interpersonal Skills:** Strong Internet Research, Excellent Verbal, Written, and Quantitative Skills, Time Management and Prioritization Abilities, Effective Presentation and Negotiation Skills , Active Listening, Patience, Adaptability, Networking

Work Experience

Technical Application Engineer | Fivesky LLC, Alpharetta, GA **July 2023 – Present**

- "Led security operations across the SDLC Process and application development process, consistently mitigated vulnerabilities by 85–90%. successfully conducted assessments, identified and resolved 98% of issues with web app source code and 95% of major mobile app vulnerabilities, with a 90% implementation rate.
- Conducted comprehensive assessments of the security architecture, identified risks, and worked with stakeholders to establish mitigation plans, assuring a robust Protection of high-value asset systems and networks. Promoted a pro-active approach to security and risk management by regularly Monitoring and reporting Progress to management.
- Contributed to the implementation of strong AWS Cloud security measures for application deployment, resulting in an outstanding 99% reduction in security vulnerabilities. This achievement was accomplished through the effective configuration of Web Application Access Control Lists (WACLS) and continuous monitoring.
- Engaged with project managers, ITSO's, Security Design Teams and subject matter experts to create comprehensive plans for aligning acquisitions with company-established security standards. Achieved a flawless 100% compliance rate with industry-leading security practices by proactively handling auditing requests and maintaining meticulous documentation efforts.

Network Security Engineer | Adhvaithsri LLC, India **June 2020 – July 2022**

- Hardened operating systems & created firewall for 95% coverage, including port-based restrictions, IPS, and Web filters.
- Developed correlation rules for SIEM, reviewed log forwarding solutions from network devices to ArcSight central logging for alerting and security monitoring and demonstrated expertise in Splunk for investigating logger events linked to security incidents.
- Managed incoming intrusion alerts using Sourcefire, SNORT IDS, and SPLUNK SIEM while also implementing standardized Splunk Phantom SOAR POV deployment, configuration, and maintenance across 90% of UNIX and Windows platforms.
- Conducted Web Application Security Assessments, Mobile Application Security Assessments, and Source Code reviews following OWASP Top 10 Vulnerability Assessments and SANS guidelines for more than 50 web applications, resolving 85% of the vulnerabilities and significantly enhancing system security.
- Performed troubleshooting of TCP/IP-related problems, successfully resolving 92% of connectivity issues and reducing network downtime by 20%. Implemented detection and prevention mechanisms for various layer 3 and layer 4 attacks, including Flood attacks (TCP SYN, UDP, ICMP), Smurf attacks (UDP, ICMP), Scans (TCP FIN, NULL, XMAS, PORT), Invalid combination of TCP Flags, IP Spoofing, Teardrop, and Ping of Death, resulting in improved system security with a 86% reduction in successful attacks.

Incident Response Analyst | Adhvaithsri LLC, India **Sept 2019 – May 2020**

- Proactively monitored and investigated WAF alerts from Sourcefire and FireEye, Improved analysis of cyber threat intelligence, correlated security events, and responded to issues, resulting in a 60% reduction in incident response time. Utilized IDS/IPS to scan the network for malicious activity; assessed firewall, IPS, and IDS logs; and recommended the CIRT team to take corrective actions.
- Conducted a comprehensive security assessment and gap analysis to evaluate compliance with security standards such as PCI-DSS, NIST Cybersecurity Framework, ISO 27001, CIS controls, GDPR, and SOC 2 audit. Identified 30 areas for security control improvement and successfully implemented 10 additional security controls.
- Demonstrated expertise in strategically aligning technology solutions with the client organization's overall business strategy, while considering financial trade-offs to manage risks, operational feasibility, and application security. Possesses in-depth knowledge of Business Continuity Plans (BCP), Disaster Recovery Plans (DCP), and Business Impact Analysis (BIA).

Security Engineer Intern | Adhvaithsri LLC, India **June 2019 – Aug 2019**

- Contributed in end-to-end DLP data encryption, monitored and remedied threats and vulnerabilities from the internal and external, and worked with Cloud Service Providers (CSPs) to set up for disasters and respond to incidents. Proficiently developed web applications using HTML5, SQL programming, and SQL Server for various tasks, including blog maintenance and social networking."
- Configured RADIUS and TACACS+, AAA servers for authentication and authorization of remote VPN users, while also conducting Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and various types of penetration testing (Hybrid, Automated, and Manual).
- Worked alongside senior architects and engineers to address vulnerabilities like SQL injection, cross-site scripting, and misconfigured servers using vulnerability scanners such as Nessus and Qualys, while also performing threat modeling with Microsoft's STRIDE tool to identify threats, motives, tactics of threat actors, and suggested countermeasures to strengthen the organization's security.

Project/Coursework

Insure Hub Internship
Pen Tester - Hacking and Penetration Testing **Aug 2022 – Dec 2022**

- Security Technologies Environment: OSNIT, Nessus, Kali, Wireshark, Nmap, Metasploit, John the Ripper, Recon-ng.
- Developed & delivered security reports to senior leadership, summarizing key findings and recommendations for improvement.
- Performed extensive vulnerability scanning and penetration testing on both Windows and Linux systems using Kali Linux and tools such as Wireshark, Nmap, and Nessus.
- Conducted manual penetration testing utilizing Metasploit and Burp Suite, identifying critical security gaps and working with development teams to remediate vulnerabilities.
- Implemented a secure configuration management process, utilizing OSNIT to ensure compliance with industry best practices.
- Collaborated with cross-functional teams to perform security assessments of new software releases, conducting source code reviews and design reviews to ensure security standards were met.

Insure Hub Internship
Information Security Management **Jan 2023 – May 2023**

- Significantly simplified account creation process by 70%, maintained & protected sensitive data, performed security audits.
- Analyzed all internal security incidents, assisted in network management, and completed risk analysis and risk assessments.
- Worked closely with IT managers and provided beneficial advice to them on any cybersecurity-related issues.
- Collaborated with colleagues on the integration of new internal security controls and created a new, more efficient information security plan which Improved information security measures by 25%, Increased efficiency by 30%, Reduced security risks by 20%, and security breaches by 15%.