POSHAN BHANDARI

6283991948 | pbhandari2@hawk.iit.edu | LinkedIn | GitHub | Website | Chicago, IL

SUMMARY

Seasoned Security Analyst with extensive experience in network, web, cloud, and mobile penetration testing. Expert in utilizing SIEM tools for comprehensive threat detection and response. Capable of designing, building, and maintaining secure technology solutions, securing networks, and data. Proven skills in identity services, authentication technologies, and lifecycle management services and automation.

EDUCATION

- **Master's,** Cyber Forensics and Security | GPA: 3.9 | *Illinois Institute of Technology*
- **Bachelor's**, Computer Networking and IT Security | GPA: 4 | *Islington College Pvt. Ltd.*

PROFESSIONAL EXPERIENCE

Graduate Teaching Assistant | Illinois Institute of Tech | Chicago, IL, USA | September 2023 - December 2023

- Enhanced graduate students' understanding of vulnerability analysis and control through targeted tutoring sessions and two-hour weekly lab sessions.
- Collaborated with instructors on course material and student performance, improving the quality of the education.
- Improved student outcomes by grading programming assignments and homework exercises and offering assistance during office hours.

Cyber Security Analyst | Monal Tech Pvt. Ltd | Kathmandu, Nepal | December 2020 - July 2022

- Enhanced cybersecurity posture through rigorous vulnerability assessments and penetration tests across diverse organizations.
- Improved the banking sector's operations by leading SIEM Proof of Concept projects, optimizing log integration, alert rules, visualization, and incident response.
- Bolstered digital defenses and prevented potential data breaches by identifying and reporting critical security bugs, including SQL Injection, Password Leakage, remote code execution, and XSS to top institutions.
- Spearheaded the creation of security newsletters and reports, raising security awareness among employees.

Cyber Security Intern | Vairav Technology Pvt. Ltd. | Kathmandu, Nepal | September 2020 - December 2020

- Boosted security by monitoring network and system activity using SIEM tools and promptly responding to security incidents.
- Collaborated with cross-functional teams to ensure compliance with industry-specific security standards and regulations, including HIPAA, PCI DSS, and GDPR.
- Contributed to incident response and investigation of security breaches, performing malware analysis, and root cause analysis.

TECHNICAL PROJECT EXPERIENCE

Threat Detection and Alerting System

- Spearheaded the creation of Network Threat Detection program integrating Suricata IDS with elastic search, Logstash, Kibana.
- Designed a system that detects suspicious signatures in network traffic, generating a comprehensive web dashboard.
- Created an efficient system for swiftly dispatching alert messages to respective system administrations upon detection of threats.

Cyber Security Awareness Program Trainer

- Designed and led Cyber Security Awareness Programs in three government schools, educating students on cybersecurity and demonstrating real-life threats.
- Improved students' risk assessment skills and their ability to identify and mitigate risks, including unknown app sources and public Wi-Fi vulnerabilities.
- Conducted sessions on phishing detection, equipping students with vital digital security skills.

SKILLS & QUALIFICATIONS

Network Security, Web Security, Cloud Security, Mobile Penetration Testing, Authentication, Identity Services, Lifecycle Management Services, Automated Processes, Application-Level Security Controls, SIEM Tools, Cyber Forensics, Ethical Hacking, Risk Crisis and Security Mgmt., Compliance Standards (HIPAA, PCI DSS, GDPR), Malware Analysis, Incident Response

CERTIFICATIONS

Certified Ethical Hacker Practical | ECC1736524089