POSHAN BHANDARI

✉ Chicago, IL ☎ 628-399-1948 ✉ poshanbhandari44@gmail.com in linkedin.com/in/poshanbhandari/

Summary

- Security analyst with 4+ years of experience in information security, specialized in penetration testing (web & infrastructure), offensive security (red team activities) and vulnerability management and with a strong knowledge of security frameworks and standards such as ***Cyber Kill Chain, MITRE, NIST and ISO 27001.***
- An ***author of DeepRecon tool***, an Open-Source Intelligence (***OSINT***) security tool on ***GitHub*****.**

EDUCATION

- **Master's,** Cyber Forensics and Security | GPA: 3.9 | *Illinois Institute of Technology* | Chicago, IL ***May 2024***
- **Bachelor's**, Computer Networking, and IT Security | GPA: 4 | *Islington College* | | Kathmandu, Nepal ***Dec 2021***

SKILLS

- **Core Cybersecurity:** Security Assessments, Vulnerability & Risk Management, Incident Response, Penetration Testing, Red Team Ops, Threat Intelligence, Security Policies, Compliance (HIPAA, GDPR, PCI DSS)

- **Technical Tools: SIEM** (Splunk, ELK, LogPoint), **Pen Testing** (Burp Suite, Metasploit, Nmap, Wireshark), **Scripting** (Python, Bash, PowerShell), **Networking** (Firewalls, VPNs, TCP/IP, DHCP)

WORK EXPERIENCE

Monal Tech **Kathmandu, Nepal**

Cyber Security Analyst *December 2020 - Jan 2025*

- Led 20+ VAPT tests using **Nessus** and **Metasploit**, resolving critical flaws (SQLi, RCE) and reducing breach risks by 60%.
- Leveraged **SIEM** to analyze logs and detect threats, reducing incident detection times by 50%.
- Researched emerging threats and vulnerabilities, proactively securing the organization’s infrastructure.
- Executed regular vulnerability scans, analyzed risk levels, and recommended mitigation strategies to strengthen security posture.
- Advised on patching and server hardening to mitigate potential risks.
- Authored and distributed security newsletters, boosting employee phishing awareness by 35% (tracked via mock tests).

Vairav Technology **Kathmandu, Nepal**

Cyber Security Intern *August 2020 - November 2020*

- Monitored 50+ endpoints using SIEM tools (Splunk, Wazuh), reducing incident response time by 25% through real-time detection of phishing and malware.
- Gained hands-on experience in **network traffic analysis and attack detection**.
- Assisted in **vulnerability scanning and threat intelligence research**, identifying emerging security threats.

CERTIFICATIONS

- **CompTIA Security+**
- **Certified Ethical Hacker (Practical) ECC173652408**

PROJECTS

Graduate Teaching Assistant | Illinois Institute of Technology *Sept 2023 – Dec 2023*

- Mentored 15+ students in hands-on penetration testing labs, enhancing their practical skills and reinforcing core cybersecurity concepts.

Volunteer Experince

WinWin Labs **Plymouth, MI**

Volunteer Cyber Security Specialist *Sept 2024 - Present*

- Conducted network and cloud **security assessments,** identifying, and mitigating **high-risk vulnerabilities, including misconfigured cloud storage buckets.**
- Identified gaps in security rule sets for attack vectors like **phishing and brute force, recommending enhanced filtering and rate-limiting rules** to improve threat detection and strengthen security policies.