RAJANI SHRESTHA

Cybersecurity Analyst | Master's of Information System Security

Edmonton, Canada | ✉ stharajani886@gmail.com | ☎ 8259256959

in linkedin.com/in/rajani-shrestha59/ | github.com/shrestharajani

Professional Summary

Driven graduate student in Information System Security Management with hands-on experience in vulnerability assessments, network security, and incident response. Proficient in leveraging cybersecurity tools such as SIEM, Nmap, and Metasploit to identify, mitigate, and respond to security threats. Experienced in implementing security policies, conducting penetration testing, and ensuring compliance with security frameworks like NIST and PCI-DSS. Strong communicator with the ability to translate complex technical findings into actionable insights for diverse stakeholders. Eager to contribute to a forward-thinking security team, enhance organizational security posture, and expand my expertise in cloud security and emerging technologies.

Skills

Cybersecurity:	Vulnerability Assessment,, Incident Response, Network Security, Forensic Analysis
Compliance & Frameworks:	NIST, PCI-DSS, OWASP Top Ten
System Administration:	Active Directory, Group Policy Management, Role-Based Access Control (RBAC)
Scripting:	Python
Cloud Security:	Basic Knowledge of Cloud Best Practices (AWS EC2, Azure)
Documentation & Reporting:	Security Reporting, Technical Documentation
Tools:	PingCastle, VMWare, Nmap, Nessus, Burpsuite, Security Onion, Autopsy, Volatility, Logpoint SIEM, pfSense, Wireshark, tcpdump, netcat, Jira
Soft Skills:	Attention to Detail, Effective Communication, Problem-Solving, Team Collaboration

Work Experience

Monal Tech Kathmandu, Nepal

Cyber Security Analyst July 2022 - Aug 2023

- Conducted vulnerability assessments and penetration testing on over 20 systems, identifying and remediating critical security gaps, resulting in a 30% reduction in overall risk
- Utilized LogPoint SIEM for comprehensive network and system log analysis, enhancing the detection of security incidents and fine-tuning detection rules to minimize false positives by 15%.
- Designed and executed a phishing awareness campaign using GoPhish for the Nursing Association of Nepal, training over 30 individuals on recognizing social engineering tactics, resulting in a 60% decrease in click-through rates during follow-up assessments.
- Recommended and supported the implementation of regular Windows OS updates and security patches across client systems, strengthening system resilience and reducing potential vulnerability exposure by proactively addressing security gaps.
- Implemented email security protocols, including SPF, DKIM, and DMARC for a client organization to protect against phishing and domain spoofing; improved authentication compliance and reduced phishing incident rates by 40%.
- Collaborated with client teams to implement and enforce security policies aligned with NIST and PCI-DSS, helping organizations achieve faster compliance readiness.
- Effectively communicated technical and non-technical security insights, translating complex concepts into actionable recommendations to enhance decision-making and security posture.

Academic Projects

Incident Response & Forensic Analysis | *Kali Linux, Nmap, Metasploit, Security Onion, Autopsy, Volatility, VMWare, Metasploitable 3 ubuntu* | GitHub: incident-response-forensics

- Simulated a real-world incident by exploiting a vulnerability (ProFTPD mod_copy) on Metasploitable 3 using Metasploit.
- Captured and analyzed network traffic with Security Onion; extracted memory artifacts using Volatility and performed forensic timeline analysis via Autopsy.
- Reconstructed attack paths and traced compromised accounts, demonstrating practical incident handling and forensic analysis skills.

Penetration Testing & Vulnerability Assessment | *VMWare, Nmap, Nessus, Metasploit, Kali, Metasploitable 3 (ubuntu), Hashcat* | GitHub: penetration-testing-vulnerability-lab

- Performed comprehensive vulnerability assessments on Metasploitable 3 server using Nmap, Nessus, and Metasploit.
- Exploited critical vulnerabilities and executed privilege escalation with PwnKit.

- Conducted password cracking with Hashcat, providing actionable remediation to strengthen system security.

Active Directory Setup & Security Hardening | *Windows Server 2019, PingCastle, VMWare* | GitHub: AD-setup-hardening

- Configured Windows Server Domain Controller and File Server with Role-Based Access Control (RBAC) and Group Policy Objects (GPO) for comprehensive security hardening.
- Managed user accounts, groups, and permissions in Active Directory to enforce least privilege access and reduce security risks.
- Used PingCastle to assess Active Directory security posture, identify vulnerabilities, and implement improvements to enhance hardening score and system resilience.

Disaster Recovery & Incident Response Plan | *Risk Assessment, Business Continuity Planning*

- Designed a detailed disaster recovery and incident response plan for a restaurant's IT infrastructure, ensuring 99.9% uptime.
- Defined employee roles, performed risk assessments, and developed business continuity strategies aligned with incident containment best practices.

Cloud Security Architecture for CPQ Application | *AWS Elastic Beanstalk, EC2, S3, IAM*

- Designed and deployed a secure AWS architecture for a CPQ (Configure Price Quote) web application using Elastic Beanstalk, EC2, S3, and IAM.
- Implemented TLS encryption, role-based access controls, and auto-scaling to ensure high availability and data protection.
- Applied cloud security best practices and monitoring strategies to meet compliance and safeguard cloud workloads.

Web Application Vulnerability Assessment | *Burp Suite, FoxyProxy, OWASP Juice Shop, bWAPP*

- Assessed real-world application flaws by testing OWASP Juice Shop and bWAPP against OWASP Top 10 vulnerabilities.
- Used Burp Suite and FoxyProxy for intercepting traffic and performing XSS, SQLi, and IDOR testing.
- Created structured penetration test reports with risk analysis, exploitability metrics, and actionable remediation strategies.

Internet and Intranet Simulation Lab | *pfSense, Netcat, VMWare, Ubuntu*

- Configured pfSense firewall and Netcat tools to simulate secure internet and intranet routing between virtualized networks.
- Applied firewall policies to control and monitor IP traffic, demonstrating practical understanding of network segmentation and zero-trust principles.
- Gained hands-on experience in managing network traffic paths, packet forwarding, and rule-based security policies.

Network Eavesdropping & Traffic Analysis | *Wireshark, tcpdump, VMWare, Ubuntu*

- Captured and inspected network packets using Wireshark and tcpdump to detect unencrypted credentials and insecure protocols.
- Identified potential eavesdropping threats and documented attack surfaces via packet analysis.
- Recommended cryptographic protocols and traffic encryption strategies to mitigate data leakage and strengthen network integrity.

Practical Training

Hack The Box – Capture-the-Flag Machines

Tools: *Nmap, Burp Suite, Hydra, SQLMap, LinPEAS, John the Ripper, Linux CLI*

- Rooted 15+ machines, including Shoppy, Responder, Photobomb, MetaTwo, and RedPanda, exploiting vulnerabilities in web apps, misconfigured services, and Linux privilege escalation paths.
- Applied red team tactics, including enumeration, credential reuse, and local privilege escalation using practical CTF scenarios.
- Gained hands-on experience with exploitation tools, Linux internals, and post-exploitation techniques in realistic environments.

TryHackMe – Guided Cybersecurity Labs

Tools: *Nmap, Wireshark, OpenVPN, Metasploit, Security Onion, Autopsy, Linux CLI*

- Completed 20+ structured labs covering pentesting, phishing analysis, forensic investigation, and defensive security.

- Practiced real-world scenarios such as log analysis, vulnerability scanning, SSH access, and malware behavior analysis.
- Reinforced foundational knowledge in networking, Linux, SIEM, and web application security through interactive rooms such as Basic Pentesting, RootMe, Bounty Hacker, OhSINT, Defensive Security Intro, and Linux Fundamentals.

Education

Concordia University of Edmonton Edmonton, Alberta
Master Information System Security Management Sep 2023 – Apr 2025

National College of Computer Studies Kathmandu, Nepal
BSc Computer Science and Information Technology 2017 – 2022

Certification and Interest

- Currently preparing for **CompTIA Security+**

Volunteer Activities

CUE Career Fair 2025
Assisted with event logistics and supported career fair operations, ensuring smooth interaction between employers and students.

CAN InfoTech 2023
Represented Monal Tech, promoting cybersecurity tools and technologies, and engaging with attendees to explain and demonstrate solutions.

ICT Award 2022
Volunteered on behalf of Monal Tech, providing information on cybersecurity initiatives and showcasing company projects to event participants.