Rohan Thapa Shrestha *Security Analyst*

rohanthapashrestha@gmail.com

9863352384

Madhyapur Thimi, Bode-8

Nepali

Male

Rohan Thapa Shrestha

RohanThapaShrestha

Rohan Thapa Sth

Education

2021 – 2024 Maitidevi, Nepal
Bachelors in Computer Science (BCS)Hons
Sunway College of Kathmandu

2018 – 2020 Bhaktapur, Nepal
+2 in Computer Science
Supreme Academy

Experience

2024/06 – present Chabahil-7, Nepal
Security Analyst
Monal Tech

- Determining project requirements and developing work schedules for the team.
- Delegating tasks and achieving daily, weekly, and monthly goals.
- Conducting Penetration Testing and Vulnerability Assessment
- Training team members
- Investigating security incidents
- Threat investigation
- Liaising with team members, management, and clients to ensure projects are completed to standard.
- Identifying risks and forming contingency plans as soon as possible.
- Analyzing existing operations and scheduling training sessions and meetings to discuss improvements.
- Keeping up-to-date with industry trends and developments.
- Updating work schedules and performing
- troubleshooting as required.
- Motivating staff and creating a space where they can ask questions and voice their concerns.
- Being transparent with the team about challenges, failures, and successes.
- Writing progress reports and delivering presentations to the relevant stakeholders.
- Conducted forensic analysis of cryptocurrency transactions using tools like **Chainalysis** and **Blockchain Explorer** to trace illicit activities such as fraud, ransomware payments, and money laundering.
- Performed end-to-end vulnerability assessments on networks, systems, and applications using industry-standard tools like **Nessus**, **Qualys**, **Burp Suite**, and **Metasploit**.
- Conducted detailed penetration tests, identifying exploitable vulnerabilities and providing remediation recommendations.
- Generated comprehensive vulnerability and penetration testing reports for clients, detailing findings, risks, and actionable mitigations.
- Determining project requirements and developing work schedules for the team.
- Delegating tasks and achieving daily, weekly, and monthly goals.

2023/11 – 2024/02 Maitidevi,Kathmandu
Front-End Developer(Intern)
Coding Glory

- Built and styled responsive web pages using **HTML5**, **CSS3**, and **JavaScript**.

- Worked with **React.js** to create interactive UI components and improve user experience.
- Collaborated with the development team to fix bugs, improve layouts, and optimize website performance.
- Gained hands-on experience with version control using **Git/GitHub**.
- Assisted in converting design prototypes (Figma/PSD) into functional web pages.
- Learned basic deployment and testing processes for front-end applications.

Skills

Technical Skills

Vulnerability Assessment & Penetration Testing (VAPT)

- Nmap, OWASP ZAP, Nikto, WPScan, Burp Suite
- **Nessus** (Vulnerability Scanning – Hands-on)

Network Fundamentals & Security

- Network Models (OSI, TCP/IP)
- Network Protocols (HTTP/HTTPS, DNS, TCP/UDP)
- Network Troubleshooting Tools: ping, traceroute, netstat
- Basic Network Security Concepts

SIEM & Security Monitoring

- **Wazuh** (Basic / Lab Exposure)
- **Logpoint** (Introductory Knowledge)
- Log collection, alert monitoring, basic rule understanding

Security Automation (Learning)

- **n8n** – workflow automation (learning, hands-on)
- Automating basic tasks using triggers, webhooks, and APIs

Operating Systems

- Linux (Ubuntu / Kali): command line usage, permissions, basic system concepts
- Windows: basic system and security fundamentals

Blockchain & Chain Analysis

- Blockchain Investigation Tools:
  - Chain Reactor
  - Chainalysis
  - Breadcrumbs
- Crypto Forensics
- Wallet and transaction identification (fundamentals)

Frontend (Basic)

- HTML5, CSS3
- JavaScript (Basic)
- React.js (Basic)

Development & Utilities

- Git, GitHub
- VS Code

Soft Skills

- Problem-Solving & Analytical Thinking.
- Communication & Reporting.
- Attention to Detail.
- Team Collaboration.
- Continuous Learning.
- Ethical Mindset.

Cybersecurity Training & labs

7/12/2025 – 14/12/2025
Pulchowk, Lalitpur

Cybersecurity & VAPT Training (7-Day Intensive Programs)
Nepal Electricity Authority (*NEA*)

- Completed an **intensive short-term cybersecurity training** focused on foundational **VAPT concepts and hands-on lab exposure**

- Covered **network security fundamentals**, service enumeration, and basic vulnerability identification
- Introduced to **web application security concepts** aligned with **OWASP Top 10**
- Practiced **basic vulnerability validation** in controlled lab environments
- Learned fundamentals of **Vulnerability Assessment & Penetration Testing methodology**
- Gained exposure to **security testing tools** and their appropriate use cases

Volunteer Training Support (During Program):

- Volunteered to **assist coworkers during hands-on training sessions**
- Helped participants understand **basic networking, tool usage, and lab tasks**
- Supported troubleshooting of **common lab and environment setup issues**
- Acted as a peer resource to clarify **security concepts and practical steps**

Tools & Technologies

Nmap, Burp Suite (Intro), Nikto, Wireshark (Basics), Linux, TCP/IP, HTTP/HTTPS

Projects

VAPT

- Conducted network, web application, and mobile application penetration tests to identify security vulnerabilities and risks.
- Utilized tools like Burp Suite, Nessus, OWASP ZAP, Nmap, Metasploit, and Wireshark for manual and automated testing.
- Prepared detailed VAPT reports including risk assessments, CVSS scoring, and remediation plans for security teams.
- Provided post-assessment guidance and support to teams in implementing security patches and best practices.
- Ensured compliance with industry standards like OWASP Top 10, NIST.

SIEM

- Developed and fine-tuned custom alert rules, dashboards, and correlation searches to detect security incidents.
- Performed log analysis and event correlation to identify indicators of compromise (IOCs), malicious activity, and policy violations.
- Investigated and responded to security alerts and incidents by performing root cause analysis and providing remediation strategies.
- Integrated SIEM solutions with threat intelligence platforms to enhance detection capabilities against emerging threats.
-

Digital Forensic

- Conducted digital forensic investigations involving cryptocurrency fraud, insider threats, malware analysis, and data breaches.
- Utilized forensic tools such as Autopsy, EnCase, FTK, Magnet AXIOM, and Wireshark to collect and preserve digital evidence.
- Investigated blockchain transactions to trace cryptocurrency theft, money laundering, and illicit activities using tools like Chainalysis and Elliptic.
- Created forensic reports with detailed findings, timelines, and evidence artifacts, supporting incident response and legal investigations.
- Collaborated with law enforcement agencies and legal teams to provide forensic evidence and expert testimony in cybercrime cases.