SUCHAN MADHIKARMI

+977 9866297150
suchanmadhikarmi123@gmail.com
github.com/SuchanMadhikarmi
linkedin.com/in/suchanmadhikarmi
portfolio: suchanmadhikarmi.com.np

EDUCATION

- Bachelor of Information Technology
  Himalayan Whitehouse International College, Kathmandu, Nepal
  Expected Graduation: [2026]
  Currently in 3rd Year
- Cyber security and AI
  Self-Learning & Online Platforms (TryHackMe, Hack the Box, Coursera and Youtube)
  Duration: [2022 – Present]

CERTIFICATIONS

Google Cybersecurity Professional Certification
ISC2 Certified in Cybersecurity(CC)
Defensive Security Operation and Cyber Risk-Cybrary
Cisco Networking Basics
Getting Started with Cisco Packet Tracer
HubSpot Email Marketing Certificate

PROJECTS

Project: SOC Automation Project
Source: github.com/SuchanMadhikarmi/SOC
Platforms and Technology Used: Wazuh, Shuffle, The hive

Project: Honeypot Deployment and Threat Visualization
Source: github.com/SuchanMadhikarmi/HoneypotVM
Platforms and Technology Used: Azure Virtual Machines, Microsoft Sentinel (SIEM)

Project: File Integrity Monitoring with Wazuh
Source: https://github.com/SuchanMadhikarmi/FIM-using-Wazuh
Platforms and Technology Used: Wazuh

Project: Phishing Simulation using Gophish
Source: https://github.com/SuchanMadhikarmi/Phising-simulation
Platforms and Technology Used: Gophish and Railway

Project: Splunk Log Analysis
Source: github.com/SuchanMadhikarmi/Splunk
Platfroms and Technology Used: Splunk

Project: Keylogger in Python
Source: github.com/SuchanMadhikarmi/Keylogger

Platforms and Technology Used: Visual Studio Code, Python

EXPERIENCE

Cybersecurity Projects and Hands-on Labs (Self-initiated)

4/6/2022 - Present

- **Network Traffic Analysis with Wireshark & TCPdump**
  Conducted detailed network traffic analysis using Wireshark and TCPdump to identify vulnerabilities and detect malicious behavior in packet capture. Gained experience in network forensics and real-time attack monitoring.
- **Packet Capture Challenge Analysis (Blueteamlabs)**
  Participated in guided packet capture challenge from Blueteamlabs.online, identifying network intrusions. Developed skills in network analysis, incident detection and vulnerability identification.
- **Vulnerability Assessment with Nessus**
  Perfomed vulnerability assessments using Nessus, identifying system weakness and potential security risks. Gained hands-on experience with vulnerability scanning and risk management.
- **MITRE ATT&CK Framework & Cyber Kill Chain**
  Gained familiarity with the MITRE ATT&CK framework and Cyber Kill Chain model to identify cyberattack stages, map attack vectors, and develop effective detection strategies**.**
- **Webshell Detection and Exfiltration Analysis**
  Participated in a cybersecurity lab focused on webshell detection and data exfiltration attempts,

Telstra - Cybersecurity Job Simulation

- Investigated network security threats and developed response strategies.
- Performed log analysis to detect and prevent cyber threats.

MasterCard - Cybersecurity Job Simulation

- Conducted phishing campaigns to assess security awareness and response.
- Analyzed security incidents and recommended mitigation strategies.
- Performed risk assessments to identify potential vulnerabilities.

SKILLS AND TECHNOLOGIES

- **Wireshark** – Moderate network traffic analysis and packet capture techniques.
- **Nessus** – Moderate vulnerability scanning and risk assessment.
- **Microsoft Sentinel** – Moderate experience in attack monitoring and threat visualization.
- **TCPdump** – Moderate network traffic capture and analysis.
- **Metasploit** – Moderate understanding of penetration testing and exploitation techniques.
- **Splunk** – Moderate experience in log analysis, monitoring, and threat detection.
- **Static Malware Analysis** – Moderate skills in analyzing malware by studying its code without executing it.
- **Dynamic Malware Analysis** – Moderate experience in analyzing malware in a controlled, executable environment to observe behavior.
- **Virtual Machines** – Good knowledge of configuring and managing virtual machines for testing, penetration testing, and security configurations.
- **Microsoft Azure** – Experience in configuring cloud-based environments, including setting up virtual machines and basic cloud security.
- **Atomic Red Team** – Moderate understanding of simulating adversary tactics, techniques, and procedures (TTPs) to improve detection and response strategies.

- **Incident Response**: Proficient in using the MITRE ATT&CK framework to identify, map, and analyze threat behaviors
- **Threat Analysis**: Skilled in leveraging MITRE ATT&CK techniques to enhance threat detection and develop adversary simulation strategies.
- **Cyber Kill Chain Framework**: Proficient in applying the Cyber Kill Chain to analyze and respond to cyberattacks.