PAWAN POUDEL

CYBERSECURITY STUDENT | OFFENSIVE SECURITY | NETWORK SECURITY | SECURITY RESEARCH

CONTACT

pawanpoudel741@gmail.com

9745280006

Kathmandu, Nepal

github.com/itspowerr

TECHNICAL SKILLS

Networking
TCP/IP, DNS, DHCP, ARP, VLAN Concepts, HTTP/HTTPS, Network Enumeration, Packet Analysis

Security Tools
Nmap, Wireshark, tcpdump, curl, netcat, SSH, Metasploit, Snort

Operating Systems
Linux, macOS, Windows

Programming & Scripting
Python, Bash, JavaScript, FastAPI

Web & APIs
REST APIs, HTTP/HTTPS, JavaScript Analysis, API Enumeration, Authentication Flow Analysis

Infrastructure & DevOps
Docker, PostgreSQL, Git, Linux Administration, Basic Cloud/VPS Deployment

Security Reporting
Vulnerability Documentation, Evidence Collection, Technical Reporting, Responsible Disclosure

LANGUAGES

- **English** – Professional Working Proficiency
- **Nepali** – Native

INTERESTS

- Offensive Security
- Vulnerability Research
- Network Security
- Web & API Security
- Reverse Engineering
- Security Automation
- Digital Forensics & OSINT

PROFESSIONAL SUMMARY

Cybersecurity-focused Computer Science student with hands-on experience in network reconnaissance, web and API analysis, vulnerability research, reverse engineering, and security assessment. Experienced in analyzing real-world systems, identifying security weaknesses, documenting technical findings, and developing proof-of-concept tooling. Strong interest in offensive security, penetration testing, vulnerability research, and network security. Seeking a cybersecurity internship where I can apply practical skills while developing professional security assessment experience.

PROJECTS & SECURITY RESEARCH

Nokia GPON Router — Reverse Engineering & Security Research

Independent Research

- Reverse engineered the authentication mechanism of a Nokia G-0425G-B GPON router.
- Documented RSA + AES hybrid encryption used in authentication process.
- Mapped more than 108 backend API endpoints through JavaScript and HTML analysis.
- Identified security weaknesses including hardcoded CSRF-related values, legacy SSH (ssh-rsa), outdated kernel, and TR-069 misconfigurations.
- Developed Python client skeleton for programmatic router interaction.

Campus Network Security Assessment

Independent Research — IIMS College

- Conducted passive reconnaissance on student WiFi infrastructure.
- Discovered HTTP captive portal exposing credentials in transit.
- Identified lack of client isolation (200+ devices visible).
- Documented MD5 password hashing with hardcoded salt in JavaScript.
- Mapped infrastructure: MikroTik routers, IIS server, SMTP mail server.
- Tested DNS tunneling (iodine) as proof-of-concept.
- Produced complete security assessment report.

Phishing Campaign Analysis & Takedown

Independent Research

- Identified and analyzed BigMart impersonation phishing campaign.
- Reversed mobile-only phishing application (JavaScript obfuscation).
- Mapped full infrastructure: domains, hosting, tracking backends.
- Documented viral spread mechanism via WhatsApp/Telegram.
- Filed abuse reports with Cloudflare, registrar, and Nepal Cyber Bureau.

ISP TR-069 Vulnerability Research

Independent Research

- Extracted TR-069 ACS credentials from own router firmware.
- Identified unencrypted HTTP management channel.
- Documented potential for mass router compromise via shared credentials.
- Produced responsible disclosure documentation.

SELECTED TECHNICAL PROJECTS

FreeLedger — Blockchain-Based Freelance Escrow Platform

Capstone Project

- Built a decentralized freelance escrow platform using React, FastAPI, PostgreSQL, Ethereum/Hardhat, and IPFS.
- Implemented wallet authentication, milestone management, dispute handling, and blockchain event processing.
- Designed REST APIs with FastAPI and containerized the application using Docker.
- Worked with security-sensitive components including authentication, authorization, blockchain transactions, file storage, and API communication.

Security & Network Tooling

- Network reconnaissance and enumeration using Nmap.
- Packet analysis with Wireshark and tcpdump.
- Linux security tooling and network diagnostics.
- Python & Bash scripting for automation and PoC tools.
- Hands-on with protocols, web apps, APIs, and auth flows.

EDUCATION

Bachelor of Computer Science (Hons) – Cyber Security
IIMS College, Kathmandu, Nepal
Affiliated with Taylor's University

Relevant Coursework:

- Computer Networking
- Operating Systems
- Cybersecurity
- Object-Oriented Programming
- Data Structures & Algorithms
- Web Technologies
- Distributed & Cloud Computing
- System Fundamentals

LEARNING & DEVELOPMENT

- Hands-on labs in network scanning and enumeration.
- Self-study: OWASP Top 10, Linux administration, Python scripting.
- Independent vulnerability research and reverse engineering.
- Experience documenting findings and preparing responsible disclosure reports.

AVAILABILITY Available immediately for on-site internship in Kathmandu.