PRAYUSH HADA

+977 9841281920 | reachprayush@gmail.com | linkedin.com/in/prayush-hada | github.com/Itsjustme27 | prayush.hashnode.com | Bhaktapur, Nepal

OBJECTIVE

Cybersecurity professional with hands-on experience in SOC operations, detection engineering, and penetration testing, building toward a focus on vulnerability research and systems/kernel security through structured study and independent low-level systems programming. Currently SOC L1 Analyst at CryptoGen Nepal and a founding member of Y3ti@Sec, a Nepal-based CTF team competing internationally in pwn, web, reverse engineering, and forensics.

EXPERIENCE

SOC L1 Analyst **Dec 2025 – Present**
CryptoGen Nepal *Kathmandu, Nepal*

- Monitor, triage, and investigate security events from SIEM, firewalls, and IDS/IPS — determine scope/impact and document findings in detailed incident reports
- Automate incident-handling workflows, including scripts that programmatically detect and assign alerts via SIEM APIs, resulting in ~85% average reduction in Mean Time to Detect (MTTD)
- Develop and tune detection and monitoring rules across LogPoint and FortiSIEM to reduce false positives and improve alert accuracy
- Work within NIST/ISO 27001-aligned SOC processes for incident handling and reporting
- Participate in vulnerability assessments; track findings and coordinate remediation with system owners
- Troubleshoot SIEM agent deployment and connectivity issues across mixed Linux environments (Rocky Linux, RHEL, Debian-based systems), ensuring consistent log collection

Founding Member **May 2025 – Present**
Y3ti@Sec

- Core CTF player focusing on pwn, web, reverse engineering, forensics, and SIEM
- Deployed and maintain a GZCTF-based competition platform (ctf.yeticyberops.com.np) on a Dokploy/Traefik VPS stack.
- Hosted Kavach CTF, an inter-college competition run jointly with NCIT College, on the platform
- Developed and maintained the team's website and internal resources
- Competed in international events such as BlitzCTF, DUCTF, and Hack A Flag, ranking among the top in Nepal
- Positioned 4th on Nepal's CTF team leaderboard according to CTFtime

Cybersecurity Intern **Jan 2025 – Feb 2025**
Sapience Edu Connect

- Set up and configured a security lab with Metasploitable and Kali Linux for vulnerability analysis
- Exploited a vsftpd vulnerability using Metasploit and performed privilege escalation
- Documented exploitation steps and mitigation measures for training purposes

SECURITY RESEARCH

Stored XSS — mbmmgt.com

- Discovered a stored XSS vulnerability in the user registration flow; injected payloads persisted and executed on every subsequent dashboard load. Reported and confirmed fixed

Critical Information Disclosure — mbmgetaway.com (Laravel)

- Identified a production Laravel deployment running with debug mode enabled, exposing a full stack trace with sensitive configuration data. Reported and confirmed fixed

PROJECTS — SYSTEMS & LOW-LEVEL PROGRAMMING

ARP Spoofing/Detection Toolkit — *C, Raw AF_PACKET Sockets, libpcap*

- Built a toolkit in C for detecting and simulating ARP spoofing using raw sockets and libpcap

DNS_TOOL (2024) — *C, Raw Sockets*

- Implemented a DNS resolver from scratch in C, following RFC 1035

LAN2LANd (2025) — *Rust, TCP Sockets, Zenity (Linux)*

- Developed a cross-platform LAN file transfer utility with a multithreaded receiver for concurrent transfers

PROJECTS — SECURITY ENGINEERING

YetiNELv2 — *Real-time log ingestion, WebSockets, JWT/RBAC*

- Building a production mini SIEM with real-time log ingestion, a WebSocket-based live dashboard, and RBAC/JWT-based access control
- Designed, built, and maintained independently, end-to-end

Phishy — Advanced Phishing Simulation Platform (2025) — *Laravel 11, PHP 8.4+, MySQL/PostgreSQL, Bootstrap 5.3, JavaScript, Node.js*

- Built a multi-perspective cybersecurity education platform simulating Attacker, Victim, and Defender roles
- Implemented RBAC, password strength tracking, and secure authentication
- Developed real-time bot simulations for phishing awareness training with probability-based scoring

EDUCATION

Bachelor in Computer System and Information Technology — **08/2023 – 08/2027**
Medhavi College, Pokhara University — *Kathmandu, Nepal*

+2 Level — **04/2021**
Chanakya College of Management — *Bhaktapur, Nepal*

SKILLS

Offensive Security & Exploitation: Metasploit, Burp Suite, gdb, radare2, Wireshark, Nmap, Tcpdump, ExifTool, steghide
Defensive / SOC & SIEM: Wazuh, LogPoint SIEM, FortiSIEM
Networking & Systems: LAN/WAN, DNS, Routing, IP addressing, Netcat, libpcap, raw sockets
Programming Languages: Python, JavaScript (ES6+), Bash, PHP, C, C++, Java, PowerShell, Rust
Other Technical: Docker, Git, GitHub, REST APIs, Linux (Arch, Kali, Ubuntu Server, Rocky Linux, RHEL)

CERTIFICATES

- **Certified AppSec Practitioner (CAP)** — TheSecOps Group, April 2025 — OWASP Top 10 and web application security fundamentals
- **SOC Level 1 Certificate** — TryHackMe, Issued Feb 2026 · Expires Feb 2029 · Credential ID: THM-PN4VKGTRIZ — SIEM, Splunk, +4 additional skills
- **Pre Security Certificate** — TryHackMe, Oct 2025
- **Student SOC Program Foundations Training** — Microsoft, Sep 2025 — Cybersecurity fundamentals, Microsoft XDR, and Microsoft Sentinel
- **Linux 100** — TCM Security, April 2025
- **NASA Space Apps Challenge Participation** — NASA, Oct 2024

ADDITIONAL INFORMATION

Languages: English (B2), Nepali (Native Speaker), Japanese (Basic)

References: *Available upon request*