

# Pallavi Kathait

Kathaitpallavi164@gmail.com — LinkedIn — GitHub — TryHackMe

## Summary

Cybersecurity Specialist with practical experience in penetration testing, vulnerability assessment, and system hardening. Proficient in using tools like Wireshark, Nmap, and Metasploitable for threat analysis and network defense. Experienced in conducting real-world security audits and reporting vulnerabilities. Strong foundation in cybersecurity concepts, supported by internships in network security and software development. .

## Education

### Bachelor of Science (B.Sc.) in Computer Science

Aug 2025 – Jul 2028

Hemwati Nandan Bahuguna Central University, Srinagar Garhwal

Developing core technical skills in programming, data structures, and computer systems.

### Class XII (90%)

Mar 2021

Saraswati Vidhya Mandir

## Experience

### Cybersecurity Intern

Oct 2023 – Nov 2023

Next Gen Software Pvt. Ltd. (Remote)

- Conducted **vulnerability assessments** and provided remediation steps to strengthen system security.
- Authored detailed **incident reports** and contributed to drafting organizational security policies.
- Assisted in monitoring live systems using **SIEM dashboards** to detect anomalies and intrusion attempts.

### Internship Trainee (Java Developer)

Oct 2023 – Nov 2023

Oasis Infobyte (Remote)

- Worked with **Java Collections, JSP, and JDBC** to improve backend processing efficiency.
- Implemented **database connectivity features** with JDBC for dynamic data handling.
- Contributed to a mini-project: a **student management system**, applying OOP concepts for modularity.

### Cybersecurity Intern

Apr 2023 – May 2023

Academor (Remote)

- Gained hands-on exposure in **network security, vulnerability testing, and cyber threat analysis**.
- Strengthened understanding of **cybersecurity fundamentals and best practices**.
- Supported research into emerging cyber threats by simulating **attack scenarios** for training.

## Projects

### ALERTIX (Security Information and Event Management Tool)

- Designed and deployed a **SIEM solution** using the ELK stack, building dashboards to distinguish between productive and distractive activities while correlating logs across multiple sources in real time.
- Implemented automated log collection pipelines from multiple servers, increasing monitoring efficiency by **40%**.

### ThreatSphere ( a sandbox for safe malware execution and behavior analysis)

- Built ThreatSphere, a sandboxed malware analysis environment that safely executes and monitors ransomware behavior in isolated systems.
- Developed a Flask + MongoDB backend to capture, store, and visualize malware activity logs for research and educational purposes.

## Skills

Cybersecurity Tools	Google Dorking, Metasploitable, SIEM, ELK Stack
Programming	Python, C, Shell Scripting
Operating Systems	Windows, Linux (Ubuntu, Kali)
Networking	TCP/IP, Wireshark, Nmap
Other	CTF Participation, Bug Bounty Hunting

## Certifications

- Networking Basics, Introduction to Cybersecurity, Computer Hardware Basics (Cisco)
- CASA (APISec University)
- CTIA (EC-Council)