

## Hands on Training

---

### Self-Learning & Practical Experience

- Gained hands-on experience in **Linux system administration**, including **user management, permissions, and security**.
- Studied **CompTIA Security+ and Linux+ topics**, including **network security, encryption, and threat management**.
- Practiced **penetration testing fundamentals** using **Kali Linux, Nmap, Metasploit, and Burp Suite** in lab environments.
- Explored **networking concepts** such as **IP addressing, subnetting, and firewall configuration** using UFW and iptables.

## Projects

---

### Cybersecurity Threat Detection & Response / *Snort, Wireshark, Splunk, Python*

October 2024 - December 2024

- Developed a **Network Security Monitoring (NSM) System** to detect and respond to security threats in real time.
- Configured **Snort as Intrusion Detection System (IDS)** to identify common cyber threats like DDoS, SQL Injection, and brute force attack.
- Analyzed network traffic with **Wireshark** and integrated **Splunk** for Security Information and Event Management (SIEM).
- Designed **custom Python scripts** to automate log analysis, incident reporting, and anomaly detection.
- Mapped findings to **CompTIA Security+ concepts** like **Threat Intelligence, Risk Management, and Security Operations**.

### Ubuntu Security Hardening & Automation / *Bash, Ansible, UFW, Auditd*

March 2024 - MAY 2024

- Developed an **automated Ubuntu security hardening script** using **Bash and Ansible**, following **CIS Benchmarks** and **CompTIA Linux+**.
- Configured **UFW (Uncomplicated Firewall)** to restrict unauthorized access and enforce secure firewall rules.
- Implemented **SSH hardening** by disabling root login, enforcing key-based authentication, and restricting user access.
- Set up **Auditd and Logwatch** for real-time monitoring of login attempts, privilege escalations, and system modifications.
- Used **Lynis and AppArmor** to conduct security audits, identify vulnerabilities, and enforce application security policies.

## Certificates

---

### C++ programming and DSA

July 2024

*CSE Pathshala*

### CompTIA Network+

December 2024

*Pearsons*

## Technical Skills

---

**Languages** Python, Bash, C++

**Technologies/Frameworks:** Wireshark, Metasploit, Nmap, Snort, Burp Suite, Kali Linux, Recon-ng

**Skills:** Network Security, Penetration Testing, Vulnerability Assessment, Security Information and Event Management (SIEM), Incident Response, Digital Forensics, Secure Cloud Architecture, Ethical Hacking

## Education

---

### Lovely Professional University Punjab

Jalandhar, Punjab

*Bachelors in Computer Application — CGPA: 7.82*

2022 – 2024

### D.A.V Public School

Patna, Bihar

*12th with Science — Percentage: 75.2%*

2021 – 2022

### D.A.V Public School

Patna, Bihar

*10th with Science — Percentage: 87.6%*

2019 – 2020

## Co-Curricular

---

- **Hackathon Host** – Organized and managed event logistics in college.
- **Marketing Experience** – Worked on outreach and promotions.
- **Hindustani Classical Music** – Junior Diploma in Hindustani Classical Vocal.
- **NGO Internship** – Assisted in outreach and awareness campaigns in Zakia Hamdard Foundation.