

# Divyanshu Chaudhary

India — +918736045689 —divyanshuchaudhary304@gmail.com  
LinkedIn — GitHub

## EDUCATION

**University of Petroleum and Energy Studies** , Dehradun, Uttarakhand  
B.Tech in Computer Science Engineering

May 2025

## SKILLS

- **Data Analysis & BI Tools** : Power BI, Tableau, Excel, SQL, Pandas, NumPy
- **Programming Languages** : Python, HTML , CSS , JavaScript
- **Security/Networking Tools** : Wireshark, Nmap, Burp Suite, Metasploit, Nessus, Arcsight , Autopsy , Arcsight
- **Cloud/DevOps**: AWS

## EXPERIENCE

**SkillMine Technologies** , New Delhi  
**Cybersecurity Analyst**

Jul 2025 – Present

- Monitored security events, investigated incidents, and escalated threats using SIEM tools to ensure rapid response and risk mitigation.
- Analyzed email headers, attachments, and payloads to detect and investigate phishing and malware attacks using tools like cisco threatgrade.
- Conducted vulnerability assessments and penetration testing, leveraging Qualys, Sandboxes, and malware analysis techniques to identify and remediate security vulnerabilities.

**DCM shriram ,(Lucknow,U.P.)**  
**Security Intern**

Jan 2025 – Jun 2025

- Assisted in basic monitoring of internal network activity and collected log data using tools like **Wireshark** under supervision.
- Helped the team organize and update IT policy documents and checklists for audits (ISO 27001). Supported internal email safety awareness by preparing simple phishing simulation reports and posters for employees.

## PROJECTS

**Cybersecurity E-Learning Website (Academic)**

HTML, CSS, Java

- Designed and developed a basic e-learning website to introduce core cybersecurity concepts.
- Implemented interactive webpages using HTML and CSS with Java for dynamic functionality.
- Focused on user-friendly navigation and responsive design for accessibility across devices.

**AI Web Scraper**

Python, Selenium, Streamlit, LangChain

- Created an AI-driven web scraper to extract structured data using LLMs and automated CAPTCHA bypassing.
- Streamlined data visualization through a custom UI built with Streamlit.
- Implemented automated scheduling for regular scraping and data updates.

**Honeypot Implementation**

AWS EC2, Nmap

- Deployed a honeypot and logged over 50+ unique attack attempts, aiding security pattern analysis.
- Monitored HTTP requests and transformed logs into structured data for anomaly detection.
- Configured alert mechanisms to notify on unusual traffic patterns in real time.

## CERTIFICATIONS

- CompTIA Security+ [SY0-701], 2024
- Cisco Introduction to Cybersecurity, 2024
- AWS Academy Cloud Computing Fundamentals, 2024
- TATA Forage Cybersecurity Analyst Program, 2025