AI and Data Science Internship

Welcome to the RD INFRO TECHNOLOGY internship program. We foster leadership, learning, and engagement. This program offers diverse opportunities in AI and Data Science.

RD INFRO TECHNOLOGY

About RD INFRO TECHNOLOGY

RD INFRO TECHNOLOGY

Vibrant Community
We unite individuals with shared goals and objectives.

Leadership Development
We offer platforms and resources to enhance leadership skills.

Learning & Engagement
Our focus includes continuous learning and student involvement.

Internship Overview

RD INFRO TECHNOLOGY

1 LinkedIn Profile Update

Update your LinkedIn profiles to reflect your association with RD INFRO TECHNOLOGY.

2 Task Completion

Complete any one of the assigned Android App Development tasks (Task 1, 2, or 3) at your convenience.

3 GitHub Repository

Maintain a separate GitHub repository named "RD INFRO TECHNOLOGY" for all tasks and share the link via the submission form..
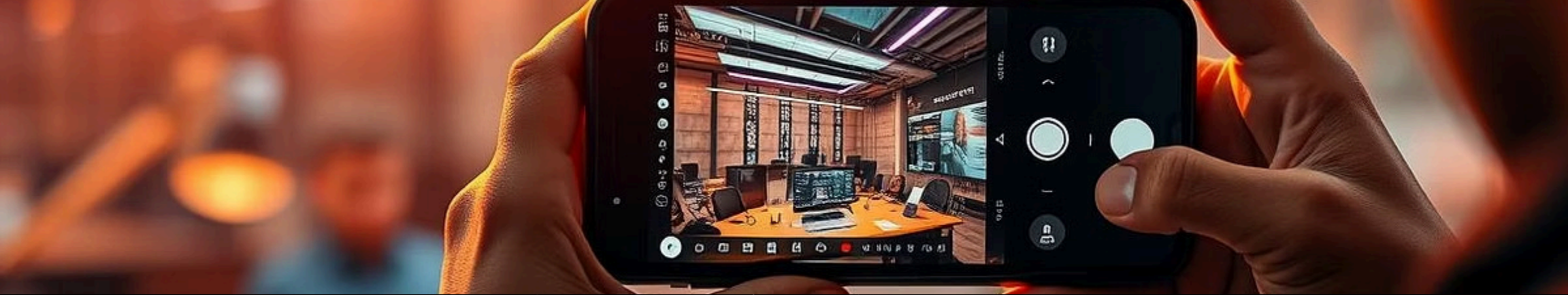
Submission Guidelines

Create a Video

Showcase your work and demo your efforts.

Host on LinkedIn

Post your video on LinkedIn to build credibility and tag RD INFRO TECHNOLOGY.

Add Hashtags

Include #RDINFROTECH and #internship in your LinkedIn posts.

Task 1: Vulnerability Assessment

- **Description**: Scan applications/systems for known security weaknesses.

- **Tools**:

- **Nmap** (network scanner)

- **OpenVAS** (vulnerability scanner)

- **How To**:

- Run `nmap -sV <target IP>` to detect open ports and services.

- Use OpenVAS to scan for known CVEs (Common Vulnerabilities & Exposures).

- Analyze the scan report and prioritize fixes.

RD INFRO TECHNOLOGY

Task 2: Web Application Penetration Testing

- **Description**: Test websites for security loopholes like XSS, SQL Injection.
- **Tools**:
- **OWASP ZAP**
- **Burp Suite**
- **How To**:
- Launch Burp Suite, set browser proxy to intercept traffic.
- Crawl the target site and look for common vulnerabilities.
- Generate automated and manual test reports.

RD INFRO TECHNOLOGY

Task 3: Network Traffic Monitoring

Description: Monitor and analyze network packets for suspicious activity.

- **Tools**:

- **Wireshark**

- **tcpdump**

- **How To**:

- Start packet capture on a network interface.

- Use filters like http, tcp.port == 80 to isolate traffic.

- Identify suspicious packets or unencrypted data.

Task 4: Password Strength Auditing

- **Description**: Test the strength of passwords within a system.
- **Tools**:
  - **John the Ripper**
  - **Hydra**
- **How To**:
  - Use John to crack hashed password files (`john <hashfile>`).
  - Test login forms with Hydra for brute-force attack simulation.

Task 5: Build a Machine Learning Model for Anomaly Detection

- **Description**: Detect unusual patterns in data (e.g., fraud or intrusion).
- **Tools**:
  - **Python (Scikit-learn, Pandas)**
  - **Jupyter Notebook**
- **How To**:
  - Preprocess dataset (missing values, normalization).
  - Train Isolation Forest or One-Class SVM model.
  - Evaluate with precision, recall, confusion matrix.

RD INFRO TECHNOLOGY

Task 5: **Facial Recognition System**

- **Description**: Recognize and identify faces from camera feed or images.
- **Tools**:
- **OpenCV**
- **dlib** or **face_recognition** (Python)
- **How To**:
- Load and encode known face images.
- Use webcam feed with `cv2.VideoCapture()`.
- Match detected faces to known encodings.

RD INFRO TECHNOLOGY

Task 7: **AI-Based Phishing Email Detector**

- **Description**: Classify emails as phishing or safe using ML/NLP.

- **Tools**:

- **Python**, **NLTK**, **Scikit-learn**

- **How To**:

- Extract features like keywords, links, sender domain.

- Train a Naive Bayes or Random Forest classifier.

- Evaluate on a labeled dataset of phishing vs. non-phishing emails.

RD INFRO TECHNOLOGY

Task 8 : **AI-Powered Log Analysis for Threat Detection**

- **Description**: Use AI to detect anomalies in server or application logs.

- **Tools**:

- **ELK Stack (Elasticsearch, Logstash, Kibana)**

- **Python (Pandas, Scikit-learn)**

- **How To**:

- Collect logs using Logstash.

- Store in Elasticsearch and visualize in Kibana.

- Export logs to Python, extract patterns, train anomaly detection models.

RD INFRO TECHNOLOGY

Ask Us for Help!

The purpose of this internship is to learn and grow. We encourage you to seek guidance. Approach tasks with professional diligence and attention.