Module 2: Case Study:
Footprinting and Reconnaissance

Problem Statement:

Imagine you are a cyber security analyst tasked with conducting a comprehensive online footprinting and reconnaissance on Intellipaat, an online education company. Your objective is to gather information from various online sources to assess the company's internet presence, identify potential vulnerabilities, and evaluate how the collected data might impact its reputation and security.

Objective:

- Conduct a comprehensive online reconnaissance of Intellipaat

- Assessing their internet presence

- Analyzing HTTP headers for server insights

- Discovering metadata-related information on a public figure or place

- Retrieving domain and email details, enumerating subdomains

- Identifying potential network weaknesses using active scanning

- Focus on reputation evaluation and security assessment

Tasks to be Performed:

1. **Internet Presence Analysis**: Explore Intellipaat's website, social media pages, and mentions in blogs and news stories to gauge their online presence and reputation. Pay special attention to any negative publicity or customer reviews that could affect the company's image.

2. **HTTP Header Inspection:** Examine the HTTP headers of Intellipaat's website. Determine how the information obtained from these headers can be valuable for footprinting and potentially revealing details about the server setup and technology in use.

3. **Metadata Analysis:** Find a public figure or a popular place and investigate how crucial information about them can be discovered in the metadata of

photos uploaded on social media. Share the specific information you retrieve.

4. **Domain Information:** Obtain details about the Intellipaat domain name, including the registrar, registration date, expiration date, and name servers associated with the domain.

5. **Email Address Research:** Investigate the support@intellipaat.com email address to discover more about the owner, searching through publicly accessible materials such as web pages, forums, and social media accounts. Share any relevant findings.

6. **WHOIS Lookup:** Perform a WHOIS lookup to find out who owns intellipaat.com and provide details such as the registrant's name, organization, email address, and phone number.

7. **Subdomain Enumeration:** List all of Intellipaat's subdomains and explain the methods or tools you used to find them.