### **CTF Topic: IP Geolocation using IP2 Location**

#### **Introduction**

IP geolocation involves determining the physical location of an IP address. This information can be used to identify where network traffic originates, which is crucial for investigating suspicious activities and understanding potential security threats. IP2Location is a web-based tool that provides detailed information about the geographic location associated with an IP address, including the country, region, city, and more.

#### 

#### **2. Tools and Requirements**

* A standard web browser to access online tools like google chrome.
* [IP2Location](https://www.ip2location.com/)

#### 

#### **3. Scenario**

Sara is investigating a series of suspicious login attempts on her company's network. By using IP2Location, she can trace the IP addresses involved in these attempts to their geographic locations, helping her identify patterns and potential sources of the attacks. This exercise will demonstrate the importance of IP geolocation in cybersecurity investigations.

#### 

#### **4. Process**

1. Open your web browser and go to [IP2Location](https://www.ip2location.com/).
2. Input the suspicious IP address(202.63.241.174) and start the lookup process.
3. Analyse the geographic information provided by IP2Location, including the country, region, city, ISP, and more.
4. Note any patterns or interesting details about the locations of the IP addresses involved in the suspicious activity.

#### 

#### 

#### **5. Let’s Begin the Challenge**

#### **Question**

* **Flag 1**: What is the city associated with the IP address 202.63.241.174?
  + **Answer**: Kathmandu
* **Flag 2**: What is the domain associated with the IP address 202.63.241.174?
  + **Answer**: subisu.net.np

**HINT**







