

International Investigations

A high-profile digital art gallery has recently been the target of cyber-attacks. The attackers attempted to access the gallery's private digital archive, potentially to leak or ransom valuable digital art pieces. Preliminary investigations have identified that the attacks originate from France. Your task, as the cybersecurity intern, is to analyze the network logs, identify IP addresses from the suspected country, and keep them for further investigation.

Prerequisites

This assignment benefits from a basic understanding of file handling in Python, particularly when it comes to reading data from files. Familiarity with opening, reading, and processing different types of files (like text files) using Python's built-in file handling methods will make the task smoother. But fret not! We will show you how to do basic file handling in python!

Background

GeoIP (Geolocation IP) technology allows the geographical location of a person or device to be determined by their IP address. It is crucial in cybersecurity for identifying the source of cyber threats, and in various other domains for content distribution and rights management.

The code snippet for calling GeoIP API is included in `international_investigations.py`!

In order to read in a file from python you can use the code snippet as shown below

```
log_file_path = 'EXAMPLEPATH/server_log.txt'    #  
Replace with your own server log path  
  
with open(log_file_path, 'r') as file:  
    content = file.read()  
    print(content)
```

With this you are able to read in the `server_log.txt` from the provided attached file!

Instructions

1. Write a Python script that reads from a provided log file named `server_log.txt`. This file contains lines of text, each including one IP address alongside other information like timestamps and request details.
2. Use the provided code attached `international_investigations.py` to query geolocation information by IP address:
3. Your task is to add on to the code so that it can filter and report any IP addresses that trace back to France as these are considered suspicious in the context of your investigation.

To submit

Submit your code in a python script along with a text file containing a brief report of the IP addresses that have been flagged as originating from France

