Graduate Project 1:

The Log Analyst
Please complete the following for submission as project 1
DUE BY: Friday 10/4/2024 @ 11:00pm

Log Analysis

Introduction
You have been retained by a company as an analyst and are being asked to prepare a report on the activities of users. This report will include the usernames, IP addresses, frequency and disposition of connections. You have been provided with a single authentication log (auth.log found attached to the project and in /usr/local/src/proj1/auth.log on our course server) that represents all the data you have available to you for the purposes of this project. The following sections define the required reports. Please carefully consider what is being asked of you to ensure that you fulfill each requirement.

Report 1: Successful Authentications [required]
From the provided authentication log, you will create a report which outlines the users who are successfully logging into services, where those connections originate from and how many times the user has logged in from that location. The table should include, at minimum, the following columns:
USERNAME, SOURCE IP, OCCURENCES

Report 2: Failed Authentications [required]
From the provided authentication log, you will create a report which outlines the source of failed login attempts to services. This will include the source IP address, the username provided and the number of times this has happened. The table should include, at minimum, the following columns:
SOURCE IP, USERNAME, OCCURENCES

Report 3: Legitimate User's Failed Authentications [required]
From the provided authentication log, you will create a report which outlines the source of failed login attempts to services using legitimate user accounts (i.e. those that have successfully logged in before as found in report 1). This will include the username, source IP address, the geo-location [see geo-location details below] and the number of times this has happened. The table should include at minimum, the following columns:
USERNAME, SOURCE IP, REGION, CITY, OCCURENCES

Report 4: Attack Sources by IP [required]
From the provided authentication log, you will create a report which outlines the geo-location association with each failed entry identified in report 2 [see geo-location details below]. The table should include at minimum, the following columns:
SOURCE IP, COUNTRY, REGION, CITY, Occurrences

Geo-location Details
You have been provided with some applications on our course server that can complete the lookup. In the event that an IP does not appear in the database, the record will show a '-' value. There is one script that produces results for both IPv4 and IPv6 addresses which can be used by feeding an IP address to the script on the command line. There is one script that produces a result for both IPv4 and IPv6, but takes the name of a file on the command line to process one line at a time. The final script takes as input, a file formatted with an IP,USERNAME,Occurrences and outputs one that has IP,USERNAME,Occurrences,Country,Region,City.
You are welcome to take a copy of the script and edit in any way you would like to meet your needs.
IP by CLI:

```
/usr/local/src/ip2location/lookup-v4-v6-brief.py 8.8.8.8
IP,Country,Region,City
8.8.8.8,US,California
```

No entry exists:

```
/usr/local/src/ip2location/lookup-v4-v6-brief.py 2606:483:988:12::1
IP,Country,Region,City
2606:483:988:12::1,-,-,-
```

Private Addresses:

```
/usr/local/src/ip2location/lookup-v4-v6-brief.py 192.168.100.201
IP,Country,Region,City
192.168.100.201,RFC1918,RFC1918,RFC1918
```

IP by File:

```
Using a flat text file with one IP per line called ip-list:
8.8.8.8
2001:4860:4860::8888
2606:483:988:12::1
192.168.100.201
fe80::1

/usr/local/src/ip2location/lookup-v4-v6-brief-file.py ip-file
IP,Country,Region,City
8.8.8.8,US,California,Mountain View
2001:4860:4860::8888,GB,England,Upper Clapton
2606:483:988:12::1,-,-,-
192.168.100.201,RFC1918,RFC1918,RFC1918
fe80::1,LinkLocal,LinkLocal,LinkLocal
```

Report by File:

```
Using a flat text file with one IP entry per line called report-list:
8.8.8.8,cschmit,12
2001:4860:4860::8888,sstevenson,32
2606:483:988:12::1,root,387
192.168.100.201,cad,38
fe80::1,joe,12

/usr/local/src/ip2location/lookup-v4-v6-report-file.py report-list
IP,Country,Region,City
8.8.8.8,cschmit,12,US,California,Mountain View
2001:4860:4860::8888,sstevenson,32,GB,England,Upper Clapton
2606:483:988:12::1,root,387,-,-,-
192.168.100.201,cad,38,RFC1918,RFC1918,RFC1918
fe80::1,joe,12,LinkLocal,LinkLocal,LinkLocal
```

Grading as follows:

- Each report has a value of 25pts - requires a complete report, including all the required columns and the appropriate number of rows.
- TOTAL - 100pts for completing all 4 reports

You must submit your findings via Sakai as 4 separate reports. The format can be either PDF or a spreadsheet format of your choosing. The filenames must be 447-LASTNAME-R[1-4].xxx (where the LASTNAME is your last name, the digit following the 'R' is the report number from above and the xxx is the file extension for the format you have chosen).