# NSSA221 Systems Administration I

# Scripting Assignment 04 – Attacker Report

**The Basics:**

The security team needs a script to generate a report on server login attempts. This report will analyze the system log file, highlighting IP addresses with ten or more failed login attempts. It should include the number of these attempts, their countries of origin, and the report's date. This script will help identify potentially compromised servers across the organization.

**Script Requirements:**

Create a Python 3 script named "*attacker\_report.py*" for use on the Rocky 8 VM in RLES, stored in the */home/student* directory. This script, meant for the enterprise environment, will be assessed by the instructor or teaching assistant based on its functionality and adherence to the specified requirements. Scoring will be guided by "*Table 1 – Script Grading Rubric*." The script's compatibility with personal laptops is not a concern for your supervisor.

**Additional Information:**

For your script monitoring remote login attempts on the organization's servers, use the provided "*syslog.log*" file from myCourses, not the local system logs. Download this file to the /home/student directory, where your script will be located. You'll need to install two Python packages to associate IP addresses with their countries of origin. The output, while not needing to match the sample in Figure 1 exactly, should be organized and readable. There's flexibility in how you display the information, as long as it's clear and structured.

The installation of the packages assumes you are using the default Python version installed on Rocky 8, version 3.6.8. If you updated the version then the commands to install these packages may be different.

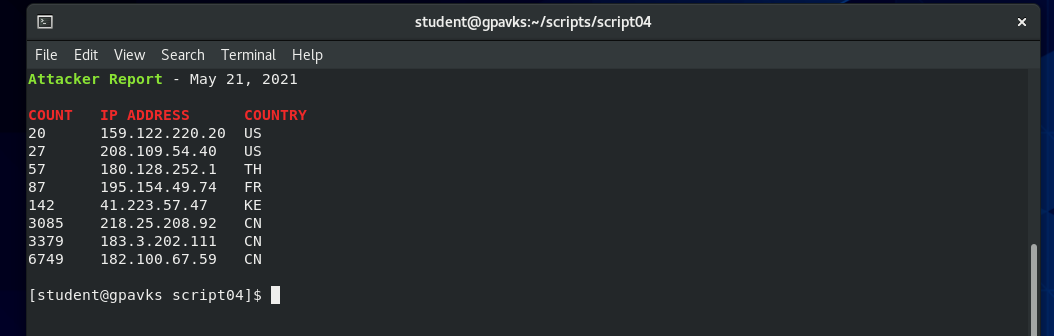
**python3 -m pip install python-geoip-python3**

**python3 -m pip install python-geoip-geolite2**

Additionally, you want to import the following module into your script.

**from geoip import geolite2**

**Figure 1** – Sample Output



**Table 1** – Script Grading Rubric

|  |  |  |
| --- | --- | --- |
| Requirements | Points | Points Earned |
| Script contains the shebang! | 2 |  |
| Script has executable permission set. | 2 |  |
| Script is commented with student’s name and date. | 2 |  |
| Script is titled “*attacker\_report.py*” | 2 |  |
| Script clears the terminal when it runs. | 2 |  |
| Report shows ten or more failed attempts. | 5 |  |
| Report shows headers, count, IP address, and country. | 5 |  |
| Report shows current date. | 5 |  |
| Count is sorted in ascending order. | 5 |  |
| Regex is used to find the IP address. | 10 |  |
| Report identifies IP address and country of origin. | 10 |  |
| The report is organized an easily readable format. | 10 |  |
| The script is sufficiently commented. | 5 |  |
| The script is written in Pythonic style. | 5 |  |
| Scripts runs with no errors. | 15 |  |
| Script is fully functional and runs as expected. | 15 |  |
| Final Grade | |  |