NSSA221 Systems Administration I

Scripting Assignment 04 – Attacker Report

The Basics:

The security team has noticed that one of its remote servers has increased failed login attempts. They suspect that other servers may also be affected and have asked you to create a script to generate a report. The report will be run on the organization's servers to analyze the system log file for the attacks. They are not looking for much. They want the report to show the IP address, the number of failed login attempts, if the number of attempts is greater than or equal to ten, the country of origin, and the report's date.

Script Requirements:

The script must be written in Python 3 and titled *"attacker_report.py."* It will be run and tested on the CentOS 8 virtual machine in your infrastructure. It must be located in the directory /home/student/scripts/script04. The infrastructure is the enterprise environment you are working in; your supervisor does not care that it can run on your laptop. The instructor or teaching assistant will run it and award points based on the requirements and overall functionality. Points awarded will be based on the criteria in *"Table 1 – Script Grading Rubric."*

Additional Information:

You are writing this script to monitor remote login attempts on the organization's servers. However, use the file, ***syslog.log***, posted to myCourses for the script, **do not** use the local device's system logs. Download this file in the same directory as the script. Additionally, you will need to install two Python packages to map the IP address with the country of origin. There is not much output needed. However, it does need to be organized and readable. See Figure 1 for sample output. It does not have to match precisely. As long as it displays the information in an organized and readable format, you have plenty of leeway in writing the script.

Install the following packages:

```
python3 -m pip install python-geoip-python3
```

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

Additionally, you want to import the following module:

```
from geoip import geolite2
```

Figure 1 – Sample Output

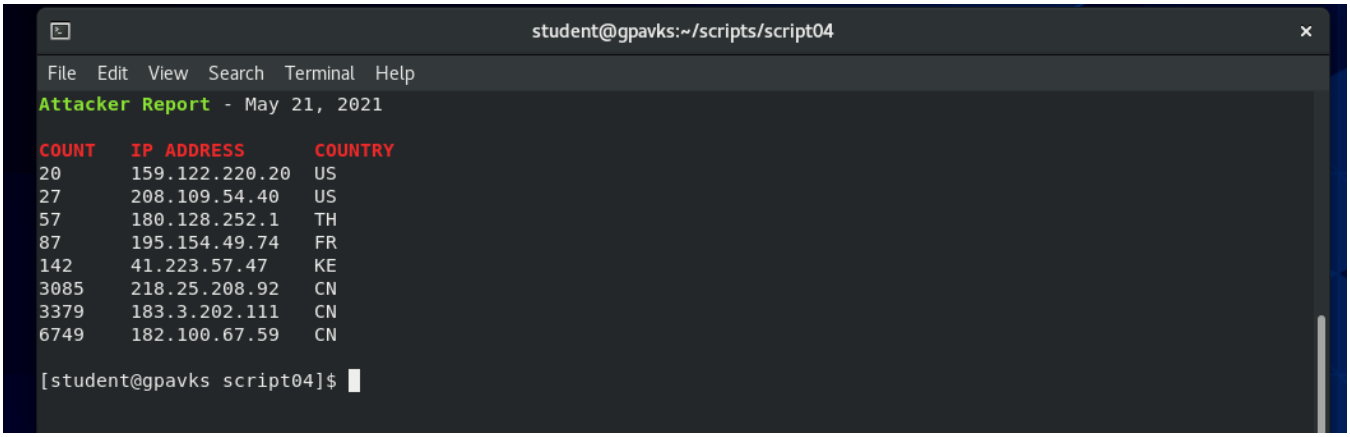

Table 1 – Script Grading Rubric

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	