Unauthorized Access Detection Script

This Python script serves as an Incident Response (IR) threat detection tool, designed to identify potential unauthorized access to user accounts based on IP location, login behavior, and suspicious post-login actions based on various detection logic (to minimize False Positives).

Features

- Detects logins from non-approved IP locations.
- Flags excessive failed login attempts (default: 3 or more).
- Identifies suspicious actions performed after a successful login (e.g., DELETE_FILE, EXPORT_DATA).
- Generates a timestamped JSON report, such as `Unauth_Access_20250504_1530.json`, containing detected issues.

Log Format (`access.log`)

The script expects the `access.log` file. Below is an example entry.

```
2025-05-04 08:01:22 IP=192.168.1.10 USER=john ACTION=LOGIN_SUCCESS
```

Sample Access Log

The sample `access.log` file includes:

- Normal user behavior.
- Brute-force attack attempts.
- Suspicious post-login activities.
- Logins from unauthorized IP addresses.

Prerequisites

- Python 3.6 or higher.
- No external libraries required.

Running the Script

1. Ensure that the `access.log` file is present in the same directory as the script.
2. Run the script:
   `python Authentication_Detection.py`

3. If any unauthorized access is detected, the script will generate a report in the form of a JSON file, such as:
   `Unauth_Access_20250504_1530.json`

Output Format

The JSON report will contain entries for each detected issue, including:

- **User**: The affected user.
- **IP Address**: The IP address from which the action was performed.
- **Country**: The country associated with the IP (based on the `IP_COUNTRY_LOOKUP` dictionary).
- **Issue**: A description of the issue (e.g., "Login from unapproved location" or "Multiple failed login attempts").
- **Actions**: A list of actions performed by the user (e.g., `LOGIN_SUCCESS`, `DELETE_FILE`).