Security Log Analysis Script

- This Python script is designed to assist organizations in analyzing system log files and identifying potential security threats. The script focuses on detecting increased failed login attempts on remote servers and generating a comprehensive security report.

Motivation

- The security team has observed a rise in failed login attempts on one of the remote servers and suspects that other servers may also be affected. To effectively address this issue, they need a tool to generate detailed reports from system log files. This script aims to provide the necessary analysis and reporting capabilities to enhance the organization's security posture.

Features

- Scans system log files to identify failed login attempts.
- Extracts IP addresses associated with failed login attempts.
- Calculates the number of failed attempts for each IP address.
- Determines if the number of failed attempts is equal to or exceeds a predefined threshold (e.g., ten).
- Utilizes geolocation data to determine the country of origin for each IP address.
- Includes the report's date to maintain a record of security analysis.

Usage

- Ensure the Python interpreter is installed on the system.
- Clone the repository or download the script file.
- Run the script using the Python interpreter.
- Provide the path to the system log file when prompted.
- The script will process the log file and generate a security report.
- Review the report to identify IP addresses, failed login attempt counts, country of origin, and potential security threats.

Requirements

- Python 3.x
- Internet connectivity for geolocation data retrieval (if applicable)

Resources

- The script utilizes the power of Python and various libraries to achieve its functionality:
- `re`: For regular expression pattern matching and extraction.
- `requests`: For fetching geolocation data based on IP addresses.

- datetime: For obtaining the current date for the report.

Disclaimer

- This script serves as a tool for security log analysis, but it does not guarantee complete threat detection or prevention. It is essential to regularly update security measures and follow industry best practices to maintain a robust security posture.

Contribution

- Contributions to this project are welcome. If you encounter any issues or have suggestions for improvements, please feel free to submit a pull request or raise an issue in the repository.

License

- This project is licensed under the MIT License. Feel free to modify and distribute the script according to the terms of the license.
- By utilizing this script, organizations can proactively identify potential security threats, analyze failed login attempts, and enhance their overall security infrastructure.