Cyber Security Project: Forensic Analysis of Logfiles Using Python.

Due 29 July 2024.

This is a Group Work.

Software needed

PyCharm or any other IDE of choice

Description

Using the Access Log file provided, perform the following forensic analysis with your group members:

1. **Identifying Suspicious Activity (Already done in the lab):**
    - Analyze the access log and identify any suspicious or potentially malicious activity, such as repeated access attempts to sensitive files, unusual user-agents, or access patterns indicative of a scanning or reconnaissance attempt.
    - Use Python to parse the log file and extract relevant information such as IP addresses, requested URLs, response codes, and user-agents.
2. **Geolocation Analysis:**
    - Perform geolocation analysis on the IP addresses found from number 1 above to determine the geographical locations of the accessing entities.

- Python libraries such as **geoip2** or web-based APIs to map IP addresses to geographic locations can be used.

3. **User-Agent Analysis:**
    - Analyze the user-agents from number 1 to identify the types of devices and browsers used by the accessing entities.
4. **Traffic Patterns and Trends:**
    - Analyze traffic patterns and trends within the access log, such as peak access times and most frequently accessed URLs
    - Python can be used to aggregate and visualize this data using libraries like **matplotlib** or **seaborn** to generate histograms, line plots, or pie charts.
5. **Security Incident Response Simulation (Presentation):**
    - Create a simulated security incident scenario using power point slides, based on the findings from the access log analysis.
    - During the presentation, this will be in form of a role-play as security analysts and develop a response plan, including steps for containment, investigation, and remediation of the security incident.

Deliverables and Points Distribution

Prepare a standard project report PDF and include the following:

- all the results of your analysis in numbers 1 to 4(including any charts or diagrams), as well as conclusions that can be derived from the analysis.
- List of predefined criteria
- Complete python script (Copy and paste your code with appropriate formatting)

Submit the single pdf to lea. Your code will be demonstrated during the project presentation.

There are a total of 100 points possible, which constitutes 30% of overall grade. Of the 100 points:

- 15 points each for the requirements in number 1 to 4 running and outputting required results, totaling 60 points.
- 20 points for the slides, presentations and role play
- 20 points for the project report.