

PDC PROJECT : LOG FILE ANALYSIS

GROUP NAME: AA

NAMES: AZHAR IQBAL , ADNAN HAYAT, SHAH NAWAZ

ROLL NO :21i\_2508, 21i\_0578,21i\_0895

Teacher : Prof ,ADIL UL REHMAN

Task1:

Detection Functions for Analyzing Activities

1. Fuzzers:

- Detect unusual or malformed requests.

- Example: High source or destination port numbers.

- Detection Logic: If the source port (orig\_p) or destination port (resp\_p) is greater than 50000, it is considered a fuzzer.

2. Analysis:

- Detect requests to known analysis tools or services.

- Example: Specific services or ports associated with analysis tools.

- Detection Logic: If the service is "http" and the destination port (resp\_p) is 80, it is considered an analysis request.

3. Backdoors:

- Detect connections to unusual ports or IPs.

- Example: Connections to high or uncommon ports.

- Detection Logic: If the destination port (resp\_p) is 5555, it is considered a backdoor connection.

4. DoS:

- Detect high volume of requests in a short period.

- Example: High orig\_bytes or resp\_bytes in a short duration.

- Detection Logic: If the duration (duration) is less than 1.0 and the original bytes (orig\_bytes) are greater than 10000, it is considered a DoS attack.

5. Exploits:

- Detect known exploit signatures.

- Example: Specific conn\_state values or unusual proto values.

- Detection Logic: If the connection state (conn\_state) is "SF" and the original bytes (orig\_bytes) are greater than 1000, it is considered an exploit.

6. Generic:

- Detect general suspicious behavior.

- Example: Unusual patterns in data transfer.

- Detection Logic: If the original bytes (orig\_bytes) are greater than 1000000, it is considered generic suspicious behavior.

7. Reconnaissance:

- Detect scanning activities.

- Example: Short duration connections to many different IPs.

- Detection Logic: If the duration (duration) is less than 0.1 and the destination port (resp\_p) is not 80 or 443, it is considered reconnaissance.

8. Shellcode:

- Detect known shellcode patterns.

- Example: Specific conn\_state values.

- Detection Logic: If the connection state (conn\_state) is "ShADfFa", it is considered shellcode.

9. Worms:

- Detect known worm signatures.

- Example: Specific proto values.

- Detection Logic: If the protocol (proto) is "tcp" and the destination port (resp\_p) is 25, it is considered a worm.

The csv files in Data set are analyzed and these feature are found to analyze the log files with malicious activity.

MPI is used in to divide the data in chunks and analyze it.  
  
  
  
Analyzing the time :

The time taken for task 1 by 2 processes is 0.06874s

The time taken for task 1 by conventional one process is 0.09775s

The time taken for task 2 by 2 processes is 0.0594s

The time taken for task 2 by conventional one process is 0.0776s

From this we analyzed that the working of mpi is very efficient for log file analysis.