VISUALISATION OF SYSTEM AUDIT LOGS

AUTHORS

Lee Kai Wen, Aloysius
Neo Ken Hong, Kelvin
Tay Zheng Yao, Schuyler
Tan Jia Le

NUS National University of Singapore

INTRODUCTION

With the increase of cyber-attacks in the recent years, incident response analyst race against time to identify crucial information that assist with halting the attacks. Analysing different types of logs and correlating them becomes vital in discovering the root cause and eradicating persistence.

OBJECTIVE

To simplify and visualise key details from system audit logs by providing a high level overview on behaviour of the processes, files interacted with and syscalls made during the runtime of the process.

REQUIREMENTS

This product works on Linux operating system, and is built on Auditd, Graphviz and Python. Visualisations will be generated based on the logs collected from auditbeat.

FEATURES

This product provides 3 main tools to visualise Auditd/Auditbeat logs.

Process Tree Visualisation
- Generates a directed graph of processes and their child processes.
- Useful for understanding flow of process creation.
- Graph includes details of running user, arguments, process path.

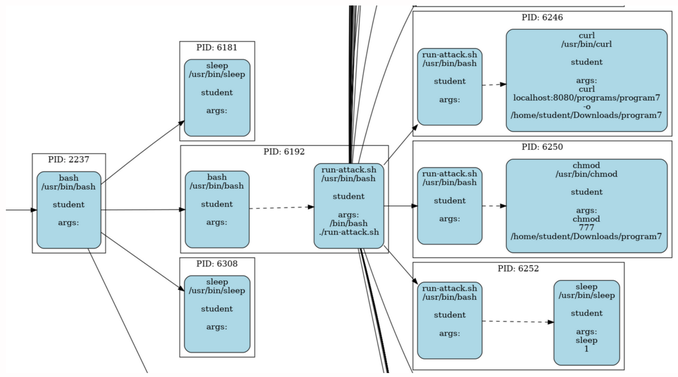
Syscalls and File Access Flowchart for Individual Processes
- Generates a directed graph of syscalls and file access for a process.
- Useful for providing high level overview into a program's execution.
- Graph includes syscall details and files associated to syscalls.

General Process-to-File Access Relationship Visualisation
- Generates a graph of files accessed by processes in the logs.
- Useful for identifying sensitive file accessed by processes.
- Graph includes file access counts and process execution details.

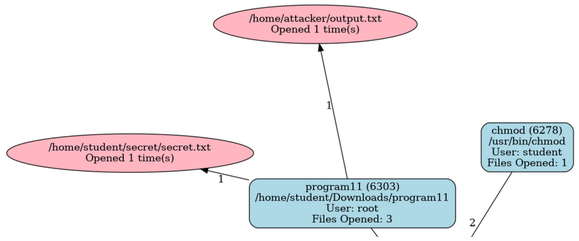
WORKFLOW

- **Collect Logs**
  - Use Auditbeat and auditd to collect Linux syscall logs
- **Analyse Process Tree**
  - Generate the process tree graph from the audit logs
  - Identify the PIDs and names of processes of interest
- **Analyse Process-File Access**
  - Generate the process-file graph from the audit logs
  - Identify the files accessed by processes of interest
- **Analyse Syscalls**
  - Generate the syscall graph of a particular PID or process name
  - Investigate the syscalls the process has executed and its respective file access

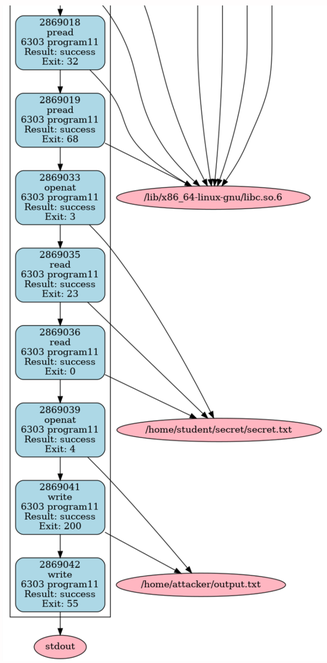
RESULTS



Process Tree Graph: Displays a graph of parent processes to its child processes, along with additional details such as the running user and its arguments.



Process File Access Graph: Displays a graph of files accessed by running processes, along with number of times opened by the process.



Syscall Graph: Displays a sequence of syscalls and the file that it is accessing.

CONCLUSION

Auditd/Auditbeat serves as an easy method of providing telemetry into how running processes interact with the kernel via the use of syscalls. By correlating log entries and back tracing, security analysts are able to draw a timeline of what had exactly occurred. In reality, numerous processes are constantly making syscalls, making it difficult to discern which pertain to malicious activities and which are legitimate. Therefore, generating visualisations based on auditbeat logs will provide a high-level overview of process behaviour and interactions on the system and assist analysts in identifying malicious programs and understand their execution.