Linux Audit Visualization Tool

James Jolly and Sam Javner

December 12, 2008

Outline

1. Introduction
2. Making Graphs
3. Displaying Graphs
4. Future Work

Why visualize audit data?

Understand the behavior of applications

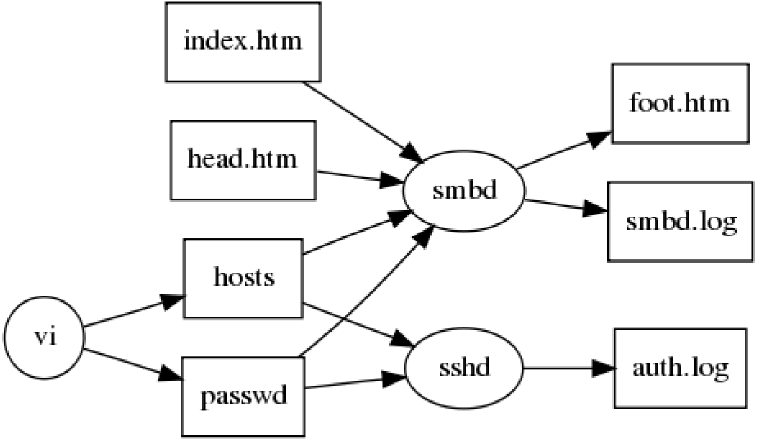
- What they influence
- How they interact with each other

The Linux Auditing Subsystem

Records system calls

- Caller
- Call name
- Files involved
- Time

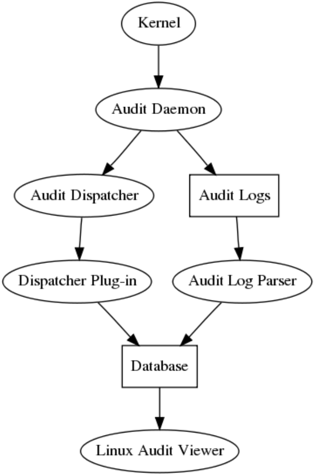
A File I/O Graph



Outline

1. Introduction
2. Making Graphs
3. Displaying Graphs
4. Future Work

Data Collection



Collection Techniques

- Granularity
- Whitelisting system calls and files
- Blacklisting executables
  - Circularity
  - Noisy processes

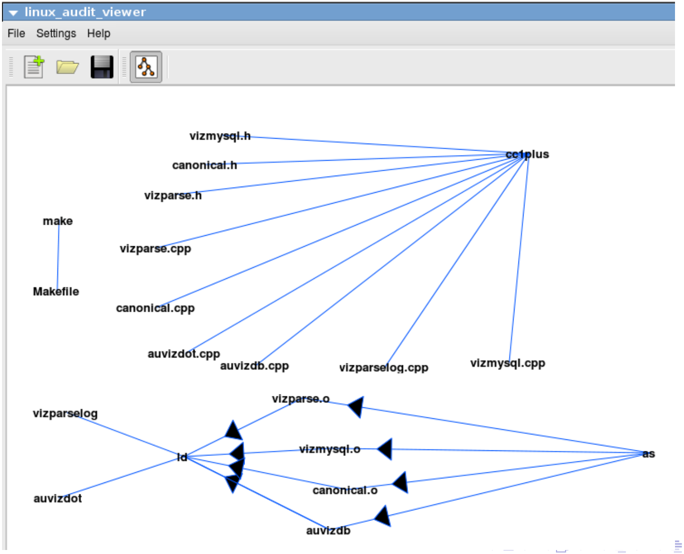
Outline

1. Introduction
2. Making Graphs
3. Displaying Graphs
4. Future Work

Objectives

- Variable time window
- Variable zoom
- Filtering mechanism
- Automatic layout
- Reorganize graph
- Take snapshots

GUI Overview



In Progress

- Flexible automatic layout
- Variable zoom
- Filter rule engine

Outline

1. Introduction
2. Making Graphs
3. Displaying Graphs
4. Future Work

Search Filters

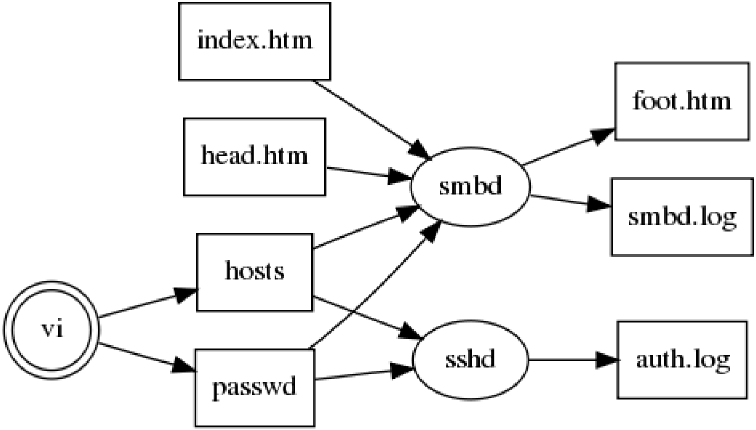


Figure: Expose k-neighborhood

Search Filters!

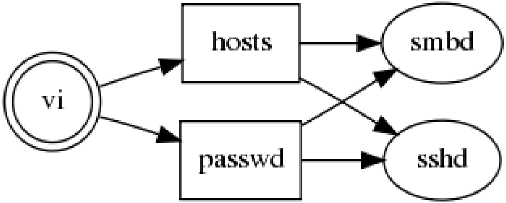
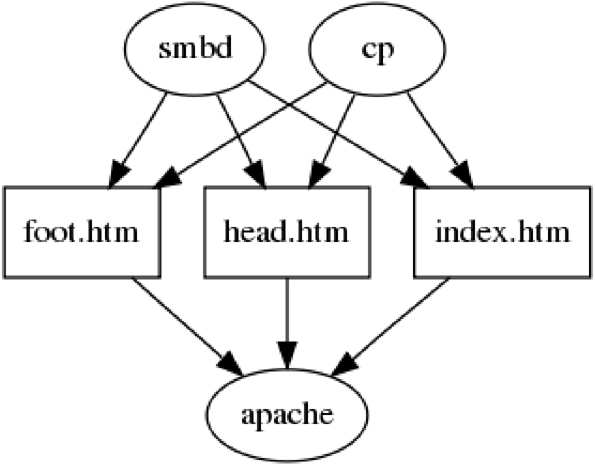


Figure: k-neighborhood of vi, k=2

Clustering



Clustering!

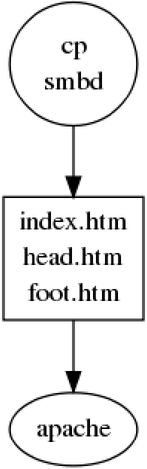


Figure: Group similar nodes

Questions?