Alternative scalable HIDS with investigation capability

FIDS - Forensic-based intrusion detection

Julian Stampfli

June 13, 2019

Table of Contents

Table of Contents

Introduction

FIDS

Summary/Conclusion

Intrusions

- What?
  - Malware
  - Hacker
  - Insider Threats
  - More Buzzwords?

Intrusions

- What?
  - Malware
  - Hacker
  - Insider Threats
  - More Buzzwords?
- Protection
  - Firewals
  - Least privilege
  - ...
- Secure

Intrusions

- What?
  - Malware
  - Hacker
  - Insider Threats
  - More Buzzwords?
- Protection
  - Firewals
  - Least privilege
  - ...
- Secure?
  - Open Ports
  - Weak Passwords
  - Insecure Applications
  - ...

Intrusion Detection

Network-Based

- Central scanning
- Uses
  - Traffic Load
  - Connections
  - Inspection
- Mainly pattern driven

Host-Based

- Distributed Scanning
- Uses
  - Processes
  - Files
  - Network Configuration
- Change driven

HIDS - FIM

Finding Changes

- Hashing to the rescue!

HIDS - FIM

Finding Changes

- Hashing to the rescue! or not?

Hashing

- Highly reliable
- Used for cryptographic use cases
- Fast?

Hashing

- Highly reliable
- Used for cryptographic use cases
- Fast? - Yes but not really.
- FIM using Hashing?
  - Tripwire - 1992 - Gone comercial
  - Aide / Samhain - Current Opensource alternatives

HIDS - FIM

Finding Changes

- Hashing
- Filesystem attributes to the rescue

TSK

The Sleuth Kit.

- Opensource
- Disk analyzis utility
- Used in forensics

Table of Contents

Introduction

FIDS

Summary/Conclusion

FIDS - Architecture

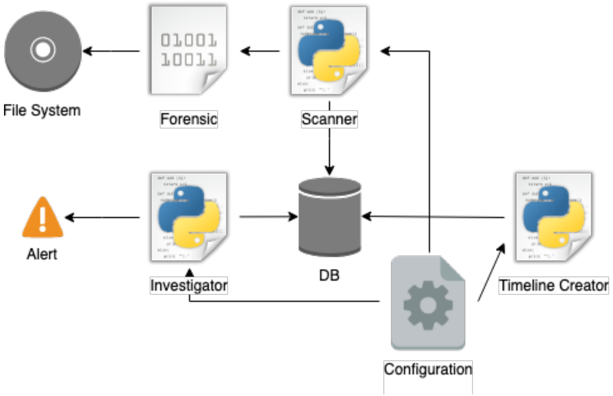

Figure: System Architecture

FIDS

- Scanner
  - Collects Data from Files System through TSK
  - Saves data to Database

FIDS

- Scanner
  - Collects Data from Files System through TSK
  - Saves data to Database
- Investigator
  - Compares Runs
  - Creates a list of anomalies
  - Based on Config

FIDS

- Scanner
  - Collects Data from Files System through TSK
  - Saves data to Database
- Investigator
  - Compares Runs
  - Creates a list of anomalies
  - Based on Config
- Timeline Creator
  - “Time Machine Format” (Forensic Timelining)

Table of Contents

Introduction

FIDS

Summary/Conclusion

Conclusion

Summary

- Fast Scans
- Intrusion Detection Possible
- Support for Forensic Investigation

Conclusion

Summary

- Fast Scans
- Intrusion Detection Possible
- Support for Forensic Investigation

Conclusion

- Risk-Based Approach
- Speed vs Reliability
- Opensource

Further Research

- Extension beyond Files
- Extensive Testing in a Live Environment

Thank you for listening / Demo?

`https://github.com/Tartori/fids`