

Alternative scalable HIDS with investigation capability

FIDS - Forensic-based Intrusion Detection System

Julian Stampfli

June 14, 2019

Table of Contents

Introduction

Forensic-based Intrusion Detection System (FIDS)

Summary/Conclusion

Table of Contents

Introduction

Forensic-based Intrusion Detection System (FIDS)

Summary/Conclusion

Intrusions

- What?
 - Malware
 - Hacker
 - Insider Threats

Intrusions

- What?
 - Malware
 - Hacker
 - Insider Threats
- Protection
 - Firewalls
 - Least privilege
 - ...
- Secure

Intrusions

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

Network-Based

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

Host-Based

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

Finding Changes

- Hashing to the rescue!

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

Finding Changes

- Hashing
- Filesystem attributes to the rescue

The Sleuth Kit.

- Opensource
- Disk analyzis utility
- Used in forensics

Table of Contents

Introduction

Forensic-based Intrusion Detection System (FIDS)

Summary/Conclusion

FIDS - Architecture

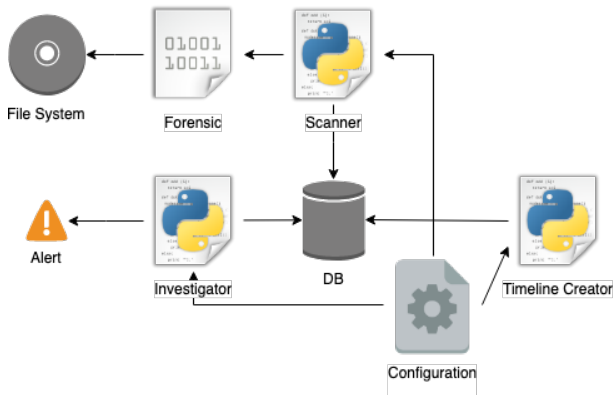


Figure: System Architecture

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

Table of Contents

Introduction

Forensic-based Intrusion Detection System (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

Further Research

- Extension beyond Files
- Extensive Testing in a Live Environment

Thank you for listening / Demo?

Come to my booth.

Code: <https://github.com/Tartori/fids>