Putting Logs on a Diet

Maximizing Impact and Effect of your Logs

10 December 2011 - BayThreat 2011 - Mountain View, CA



Presented by:
Kevin W. Lawrence
Stach & Liu, LLC
www.stachliu.com



Agenda

O V E R V I E W

- Introduction/Background
- Baseline
 - Why Log
 - Less is More
 - Targeting
- Analyze
 - Combing Logs
 - Execution
- Recap



Introduction/ Background



About Me

- Senior Security Associate for Stach & Liu
- Over eight years designing, implementing, and responding to various cyber security controls
- Alphabet Soup
 - CISSP, GCIA, GREM, GCFA, CEH



Problem Statement

Finding actionable security events within system, network, and application logs can be overwhelming due to data volume.



Baseline

What do your logs tell you?



Auditing



- Auditing
 - Compliance



- Auditing
 - Compliance
- Operational Monitoring



- Auditing
 - Compliance
- Operational Monitoring
 - Up/Down
 - Performance



- Auditing
 - Compliance
- Operational Monitoring
 - Up/Down
 - Performance
- Security



- Auditing
 - Compliance
- Operational Monitoring
 - Up/Down
 - Performance
- Security
- Solving A Problem



• Filter



- Filter
 - Before



- Filter
 - Before
 - During



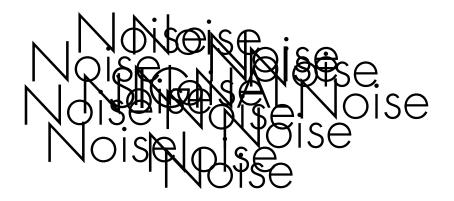
- Filter
 - Before
 - During
 - After



- Filter
 - Before
 - During
 - After
- Signal to Noise



Example





• What Do You Need



- What Do You Need
- Removing Known Good



- What Do You Need
- Removing Known Good
- What Can You See



- What Do You Need
- Removing Known Good
- What Can You Use
- Remove Excess Data



Analyze



Aggregate and Correlate



- Aggregate and Correlate
- Multiple Sources



- Aggregate and Correlate
- Multiple Sources
 - Network
 - System
 - Application



- Aggregate and Correlate
- Multiple Sources
 - Network
 - System
 - Application
- Time



- Aggregate and Correlate
- Multiple Sources
 - Network
 - System
 - Application
- Time
 - NTP
 - Time Zone



Monitor Log Flow



- Monitor Log Flow
 - Passive



- Monitor Log Flow
 - Passive
 - Active



- Monitor Log Flow
 - Passive
 - Active
- Honey Tokens



- Monitor Log Flow
 - Passive
 - Active
- Honey Tokens
 - Credentials
 - Accounts
 - Database
 - Records
 - API
 - Keys
 - Files
 - Robot.txt

Adminn00b

Credit Card Numbers

Social Network API Keys

oldadmin.php



Future Direction



Future

Integration



Future

- Integration
- Automation



Future

- Integration
- Automation
- Proactive Detection



Recap

- Baseline
 - Why Log
 - Less is More
 - Targeting
- Analyze
 - Combing Logs
 - Execution



Special Thanks

Christie Grabyan Fran Brown Vincent Liu

Questions?

For more info: Email: klawrence@stachliu.com Stach & Liu, LLC www.stachliu.com

Thank You

