Auditing Mac Logs
Overview
Dustin Udy
Information Security Office / Enterprise Security
Topics

• Unified Logging
• Oldies but goodies
• ASL Logs
• How to read logs
• Log tool
Unified Logging

- Mac OS X 10.12+
- iOS 10.0+
- tvOS 10.0+
- WatchOS 3+
- Supersedes ASL and Syslog API’s
Log locations

Unified logs are binary logs stored in two locations
- /var/db/diagnostics
- /var/db/uuidtext
Oldies but goodies

/var/log

- system.log - Still shows relevant data from third-party logs
- install.log - software install information
- third-party apps still use this location

/Library/Logs

- Third-party apps

~/Library/Logs

- Third-party apps in user home directory
/var/log/asl

- could still be valuable data going here from third-party apps. Mileage may vary
How to read logs

Favorite CLI text tool
- For the .log or .txt files

Syslog command
- For ASL files
How to read logs

Console.app
- Mileage seems to vary on what logs are returned (not my preferred tool)
- Differences between Sierra and High Sierra

Log CLI tool
- Used for the Unified Log archives
- Preferred method
Log tool

Log commands

- log stream
- log show
- log collect
- log erase - CAUTION
- log help
SSH examples

This will show a lot of data, some useful some not so useful

• log show --predicate 'eventMessage contains "ssh"' --info

Make the search more useful with processImagePath

• log show --style syslog --predicate 'eventMessage contains "ssh2"' --info

Find the failed or brute force ssh login attempts

• log show --predicate 'processImagePath contains[c] "sshd" && eventMessage contains "error"'
SSH examples

Find all of the successful ssh logins, must use the "--info" option

• log show --predicate 'processImagePath contains[c] "sshd" && eventMessage contains "Accepted" --info

Find both success and fail/brute force

• log show --predicate 'processImagePath contains[c] "sshd" && (eventMessage contains "Accepted" || eventMessage contains "error")' --info
Sudo examples

All commands from the sudo process
• log show --predicate 'processImagePath contains[c] "sudo"

Failed sudo commands
• log show --predicate 'processImagePath contains[c] "sudo" && eventMessage contains "incorrect"

- Adding --info may or may not give more logs
Questions?
Reference Material

http://macitbusiness.com/macintosh-auditing-logging/


http://www.manpagez.com/man/1/log/

https://stream.lib.utah.edu/index.php?c=details&id=12848 - Mac managers Presentation by Nic Scott

Reference Material

http://krypted.com/mac-os-x/logs-logging-logger-oh/

https://eclecticlight.co/2016/10/17/log-a-primer-on-predicates/

https://eclecticlight.co/2017/03/14/useful-filter-terms-for-sierras-logs/


https://eclecticlight.co/2018/03/20/macos-unified-log-2-content-and-extraction/

https://eclecticlight.co/2018/03/21/macos-unified-log-3-finding-your-way/