Dr Anton Chuvakin
Chief Logging Evangelist

Log Forensics

Goals

- Get a **refresher on logs** and logging
- Become familiar with **log analysis** for investigative purposes
- Learn what **"log forensics"** really is

Outline

- Log and logging overview
- A brief on Incident response and forensics
- Logs in incident investigations
- Just what is log forensics?
- Conclusions and call to action!

Logs for Cybercrime Investigations

A few thoughts to start us off …

- **All attackers leave traces. Period!** ☺
- It is just that you *don't always know* **what** and **where**
- And *almost never know* **why**
- **Logs** are the place to look, **first**

Definitions

- **Log** = record related to whatever activities occurring on an information system
- Also: alert, "event", alarm, message, audit record, *etc*

- ***standard definitions are coming soon: CEE standard by MITRE (in a few weeks)***

Log Data Overview

What logs?

- Audit logs
- Transaction logs
- Intrusion logs
- Connection logs
- System performance records
- User activity logs
- Various alerts and other messages

From Where?

- Firewalls/intrusion prevention
- Routers/switches
- Intrusion detection
- Servers, desktops, mainframes
- Business applications
- Databases
- Anti-virus
- VPNs

What Commonly "Gets Logged"?

- System or software **startup, shutdown, restart, and abnormal termination** (crash)
- Various **thresholds being exceeded** or reaching some levels such as disk space full, memory exhausted, or processor load too high
- **Hardware health** messages that the system can troubleshoot or at least detect and log
- **User access** to the system such as remote (telnet, ssh, etc.) and local login, network access initiated to and from the system, failed and successful
- User access **privilege changes** such as the su command—both failed and successful
- User credentials and **access right changes**, such as account updates, creation, and deletion—both failed and successful
- System **configuration changes** and software updates—both failed and successful
- **Access to system logs** for modification, deletion, and maybe

Log Analysis: Why

- Situational **awareness** and new threat **discovery**
  - Who is doing what on a server
- Getting more value out of the network and security **infrastructure**
  - Firewall logs for ID
- **Measuring** security (metrics, trends, etc)
  - Top users by bandwidth from firewall logs
- **Compliance** and regulations (oh, my!)
  - Report on access to credit card data in a database
- **Incident** response (<u>last, but not least!</u>)

Log Analysis: Why NOT

- *"Real hackers don't get logged!"* ☺
- Why bother? No, really …
- Too much data (>x0 GB per day)
- Too hard to do
- Is this device lying to me? ☺
- No tools "that do it for you"
  - Or: tools too expensive
- *What logs? We turned them off* ☹

Log Analysis Basics: How

- **Manual**

  'tail', 'more', etc
- **Filtering**

  Positive and negative ("artificial ignorance")
- **Summarization** and reports
- Simple **visualization**

  "…worth a thousand words?"
- **Correlation**

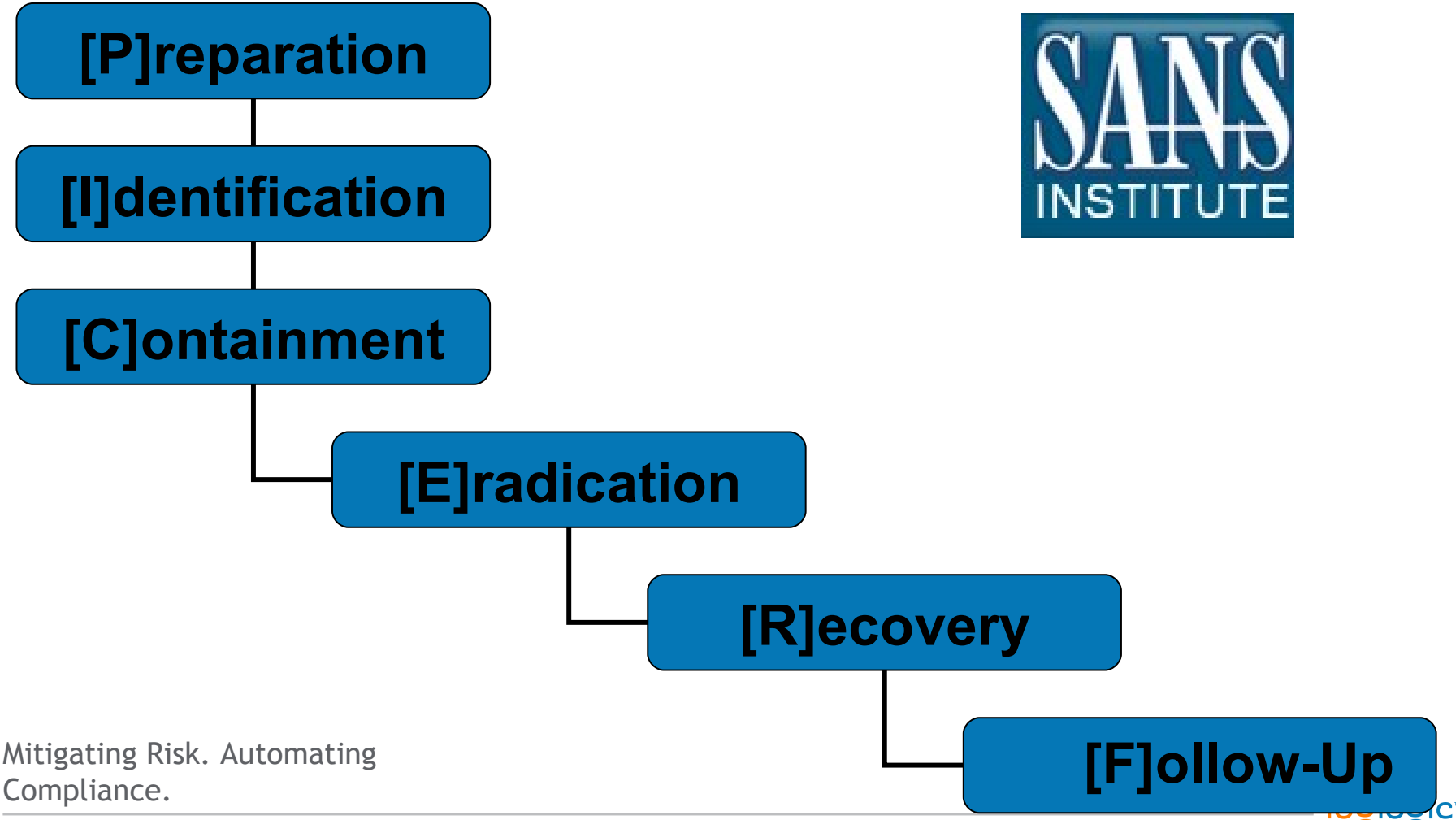
  Rule-based and other

Select Log Analysis Tools

- Log **collection**
  - Syslog-ng, kiwi, ntsyslog, LASSO, DAD, Apache2syslog, etc
- Secure **centralization**
  - Stunnel, ssh, free IPSec VPNs
- **Pre-processing**
  - LogPP
- **Storage**
  - MySQL or design your own
- **Analysis** – oooh, a tough one! ☺
  - SEC for rule-based correlation
  - SLCT for simple clustering
  - OSSEC, OSSIM and AANVAL for [*some*] intelligence
  - Swatch, logwatch, logsentry, other *match-n-bug* ☺ scripts

Logs in Incident Response

Incident Response Methodologies: SANS



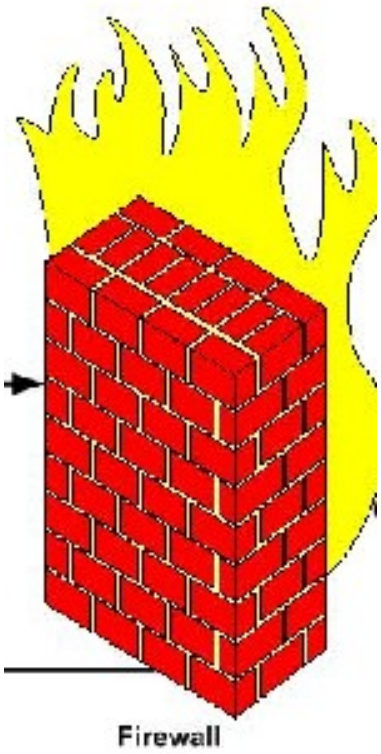
Mitigating Risk. Automating Compliance.

Logs at Various Stage of Incident Response

- **Preparation**: verify controls, collect normal usage data, baseline, etc
- **Identification**: detect an incident, confirm incident, etc
- **Containment**: scope the damage, learn what else is “lost”, what else the attacker visited/tried, etc
- **Eradication**: preserving logs for the future, etc
- **Recovery**: confirming the restoration, etc
- **Follow-Up**: logs for “peaceful” purposes (training, etc) as well as preventing the recurrence

Firewall Logs in Incident Response

- Proof of Connectivity
- Proof of NO Connectivity
- Scans
- Malware: Worms, Spyware
- Compromised Systems
- Misconfigured Systems
- Unauthorized Access and Access Attempts
- Spam (yes, even spam!)



Example: Firewall Logs in Place of Netflow

- Why Look at Firewall Logs During Incident Investigation?
- 1990-2001 – to see what *external* threats got **blocked** (in, failure)
- 2002-2006 – to see what *internal* system got **connected** (out, success)
- Thus, firewall logs is "poor man's" *netflow*…

NIDS Logs in Incident Response

- Attack, Intrusion and Compromise Detection
- Malware Detection: Worms, Viruses, Spyware, etc
- Network Abuses and Policy Violations
- Unauthorized Access and Access Attempts
- Recon Activity
- [NIPS] Block

Server Logs in Incident Response

- Confirmed Access by an Intruder
- Service Crashes and Restarts
- Reboots
- Password, Trust and Other Account Changes
- System Configuration Changes
- *A World of Other Things* ☺

Database Logs in Incident Response

- Database and Schema Modifications
- Data and Object Modifications
- User and Privileged User Access
- Failed User Access
- Failures, Crashes and Restarts

T.J.maxx® you should go™

LOOK AT YOUR LOGS! ☺

Example: And What is NOT Stolen?

- *Supposedly*, all of ChoicePoint 40 mil cards were not stolen… They just **couldn't prove they weren't.**
- Database logs as a way of *non-intrusion detection* (or, rather, confirmation of impact)

- On the other hand, TJMaxx 47 mil cards **were** stolen ☹

Log Forensics

So, What is "Log Forensics"

- **Log analysis** is trying to make sense of system and network logs
- "**Computer forensics** is application of the scientific method to digital media in order to establish **factual** information for **judicial** review."

So….

- **Log Forensics** = trying to make sense of system and network logs + in order to establish factual information for judicial review

Overall, a *bizarre* mix of **science, technology**

How Logs Help… Sometimes

If logs are *there*, we can *try* to

- … figure out **who**, **where**, **what**, **when**, **how**, **etc**

but

- **Who** as a person or a system?
- Is **where** spoofed?
- **When**? In what time zone?
- **How**? More like 'how'd you think'…
- **What** happened or what got recorded?

Who?

Man vs machine: identity fight

- Just **who is 10.1.1.2**? Do you know *him*?
- Is **jsmith.example.com** a *who*?
- Is **JSMITH** at \\JSMITH\EXAMPLE?
- Is **JSMITH authenticated** by an RSA token at \\JSMITH\EXAMPLE and also logged to another system as "jsmith" a *who*?

When?

Got timestamp? ☺ - challenges to log timing!

- Completely **false timestamp** in logs (BTW, *today is Jan 1, 1969)*
- It's **always 5PM somewhere:** which timezone are your logs in?
- Are you in **drift? Your clock** might be (*those pesky seconds turn into minutes…*)
- **Syslog forwarder** mysteries: "his" time vs "my" time
- So, which one is right? Systems with **two timestamps!**
- It got logged at 5:17AM. When did it **happen**? Log lag!

When? II

- **Sequence** of events is a critical fact! Miss the sequence and the whole "house of cards" goes …
- But! **Absolute** time is also important! How to find it?
- More "*fun*" time issues to watch for:
  - Process leaves a log records when it *exits* (log lag)
  - Stuff missing from logs altogether (a
  - Logs with out of sequence time stam

```
Directory of C:\Windows\System32\LogFiles\W3SVC1

09/27/2003  07:00 PM        1,461,370 ex030927.log
09/29/2003  07:00 PM          629,006 ex030929.log
09/30/2003  07:00 PM        1,134,950 ex030930.log
               3 File(s)    3,331,151 bytes
               2 Dir(s)  7,842,717,696 bytes free
```

Where?

- The attack came from 10.1.1.2 which belongs to Guanjou Internet Alliance, Beijng China
- The stolen data then went to 10.2.2.1 which belongs to PakNet ISP in Karachi, Pakistan
- **Result**: *Romanian* hackers attack! ☺

or

- **Result**: it was a guy from the office on the 3rd floor?

or …

How?

- **Interpretation is inherent** in answering the "how" question! Information is always incomplete!
- What is "how"?
  - How it got recorded [in logs]?
  - How we think it happened?
  - How we <u>believe</u> it happened?
  - How it happened? **<- only this is forensics**

What?

- **"False positives"** – need I say more? ☺
- Other **"lying logs"** include:
  - System errors that are corrected automatically
  - Misinterpreted log messages (*Oh my, error 4632 strikes again!*)
  - Artificially inserted logs (ever used */usr/bin/logger*?)
  - Finally, logs that *someone edited*
    - Added (log flooding)
    - Removed (log "cleaning")
    - Changed (log corruption)

Finally, Logs that Aren't: Log Security

Log security MUST be built-in up front!

- **Transmission** security (SSL, SSH, etc)
- **Storage** security (encryption [*], signing or hashing)
- No **changes**! After all, *why change logs?* ☺ WORM!
- **Access control** – "need to know" basis
- Access and *process* **logging -** log who saw the logs! [**]
- **<u>Last resort:</u>** printer + safe + armed guard

Logs Forensics Challenges: From US DoJ

"Computer Records and the Federal Rules of Evidence"

- "**First**, parties may **challenge the authenticity** of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created.
- **Second**, parties may question the authenticity of computer-generated records by **challenging the reliability** of the computer program that generated the records.
- **Third**, parties may challenge the authenticity of computer-stored records by **questioning the identity** of their author."

Conclusions

- **Turn ON Logging!!!**
- Make Sure Logs Are There When You Need Them (and need them you will ☺)
- When Going Into the Incident-Induced Panic Think *'Its All Logged Somewhere – We Just Need to Dig it Out'*
- Logs for Forensics
  - Logs can tell you things, but are they "good evidence"?
  - Extra considerations are there for forensic use of logs
  - Logs become evidence only if precautions are

More information?

Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA

anton@chuvakin.org

Chief Logging Evangelist

LogLogic, Inc

Author of "Security Warrior" (O'Reilly 2004) – www.securitywarrior.com

See www.info-secure.org for my papers, books, reviews and other security resources related to logs

Thank You for Attending!

My Tutorial on Logs in Incident Response Starts at 16:00!