Logs in Incident Response

Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA
Director of Security Research
LogLogic
anton@loglogic.com

Mitigating Risk. Automating Compliance.
Outline - I

- Incident Response Process
- Logs Overview
- Logs Usage at Various Stages of the Response Process
- How Log from Diverse Sources Help
Outline - II

- Log Review, Monitoring and Investigative processes
- Standards and Regulation Affecting Logs and Incident Response
- Incident Response vs Forensics
- Log Analysis and Incident Response Mistakes
- Case Studies (throughout...)
To Avoid DBPPT Disease 😊

Together we can bring order to galaxy
If you only knew the power of the Dark Side
➢ Force is with you — but you are not used yet
➢ Join me and I will complete your training
➢ You can destroy the Emperor (but beware of this)
   - It is your destiny
➢ I am your father
   - Search your feelings. You have the power
➢ Together we shall rule the galaxy & son
➢ Come with me. It is the only way
➢ It is your destiny!

For more info visit my webpage at www...
Incident Response Processes
Incident Response Methodologies: SANS

- SANS Six-Step Process
  - [P]reparation
  - [I]dentification
  - [C]ontainment
  - [E]radication
  - [R]ecovery
  - [F]ollow-Up
Incident Response Methodologies: NIST

○ NIST Incident Response 800-61
  1. Preparation
  2. Detection and Analysis
  3. Containment, Eradication and Recovery
  4. Post-incident Activity
Process from “Incident Response and Forensics”

1. Preparation
2. Detection
3. Initial response
4. Formulate response strategy
5. Investigation
6. Resolution and Recovery
7. Reporting
Other IH/IR Frameworks and Methodologies

- Company-specific Policies and Procedures
- Sometimes: good, bad and ugly (aka “Just put it the way it was…”)
  - Escalation trees
  - Virtual CIRT structures and call lists
  - Intra-company processes
  - Etc, etc, etc
Why Have a Process?

- **It helps…**
  - Predictability
  - Efficiency
  - **Auditability**
  - Constant Improvement

- **It shrinks…**
  - Indecision
  - Uncertainty
  - Panic! 😞
Example: Worm “Mitigation” in a Large Company...

... circa 2002 AD 😊

- Worm hits
- Panic + initial response in parallel (urgh! 😊)
- Mitigation + investigation at the same time
- Two walking steps forward and 10 running steps back...
From Incident Response to Logs
Terms and Definitions

- **Logging**
- **Auditing**
- **Monitoring**
- **Event reporting**
- **Log analysis**
- **Alerting**

- **Message** – some system indication that an event has transpired
- **Log** or **audit record** – recorded message related to the event
- **Log file** – collection of the above records
- **Alert** – a message usually sent to notify an operator
- **Device** – a source of security-relevant logs
So, What is A Log?

- Typically, a log “file” is a file that lists all actions that have occurred on a device, within an application, or on a server
- *Example*: is SNMP trap a log? Is a netflow record?
Log Data Overview

What data?
- Audit logs
- Transaction logs
- Intrusion logs
- Connection logs
- System performance records
- User activity logs
- Various alerts

From Where?
- Firewalls/intrusion prevention
- Routers/switches
- Intrusion detection
- Hosts
- Business applications
- Anti-virus
- VPNs
Devices that Log: An *Attempt* at a Comprehensive List

- Network gear: routers, switches,
- Security gear: firewall, IDS, VPN, IPS,
- Access control: RAS, AD, directory services
- Systems: OS (Unix, Windows, VMS, i5/OS400, etc)
- Applications: databases, email, web, client applications
- Misc: physical access,
- Other: just about everything with the CPU…
What Commonly “GetsLogged”? 

- System or software **startup, shutdown, restart, and abnormal termination** (crash)
- Various **thresholds being exceeded** or reaching dangerous 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 (FTP) 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 even reading
"Standard" Messages

10/09/2003 17:42:57, 146.127.94.13, 48352, 146.127.97.14, 909, 146.127.93.29, 0, 4, 3, '9 Oct 2003 17:42:57, accept, labcpngfp3, inbound, eth2c0, 0, VPN-1 & FireWall-1, product=VPN-1 & FireWall-1[db_tag={0DE0E532-EEA0-11D7-BDFC-927F5D1DECEC}; mgmt= labcpngfp3; date=1064415722; policy_name= Standard], labdragon, 48352, 146.127.93.145, eth2c0, inbound


2003-10-20|15:25:52| dragonapp-nids| TCP-SCAN| 146.127.94.10|146.127.94.13|0|0|X|------S-|0|total=484, min=1, max=1024, up=246, down=237, flags=------S-, Oct20-15:25:34, Oct20-15:25:52|

Oct 20 15:35:08 labsnort snort: [1:1421:2] SNMP AgentX/tcp request [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 146.127.94.10:43355 -> 146.127.94.13:705

SENSORDATAID="138715" SENSORNAME="146.127.94.23:network_sensor_1" ALERTID="QPQVIOAJKBN0O6K6FTNLESZ" LOCALTIMEZONEOFFSET="14400" ALERTNAME="pcAnywhere_Probe" ALERTDATETIME="2003-10-20 19:35:21.0" SRCADDRESSNAME="146.127.94.10" SOURCEPORT="42444" INTRUDERPORT="42444" DESTADDRESSNAME="146.127.94.13" VICTIMPORT="5631" ALERTCOUNT="1" ALERTPRIORITY="3" PRODUCTID="3" PROTOCOLID="6" REASON="RSTsent"
Logs at Stages of IR (SANS Model)

- **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, etc
- **Eradication**: preserving logs for the future, etc
- **Recovery**: confirming the restoration, etc
- **Follow-Up**: logs for “peaceful” purposes (training, etc)
Using Logs at Preparation Stage

- Verify Controls
- Ongoing Monitoring
- Change Management Support
- “If you know the cards, you’d live on an island” 😊

- In general, verifying that you have control over your environment
Monitoring infrastructure based on NSM philosophy: netflow + packet content + logs (NIDS, etc)

Pre- and post-incident monitoring

Useful even if deployed after the incident, but most useful if deployed prior to it
Using Logs at Identification Stage

- Detect Intrusion, Infections and Attacks
- Observe Attack Attempts, Recon and Suspicious Activity
- Perform Trend Analysis and Baselining for Anomaly Detection
- Mine the Logs for Hidden Patterns, Indicating Incidents in the Making…
- “What is Out There?”

2: 1
Example 2 FTP Hack Case

- Server stops
- Found ‘rm-ed’ by the attacker
- What logs do we have?
- Forensics on an image to undelete logs
- Client FTP logs reveals…
- Firewall confirms!
Using Logs at Containment Stage

- Assess Impact of the Infection, Compromise, Intrusion, etc
- Correlate Logs to Know What You Can [Still] Trust
- Verify that Containment Measures Are Working
- “What Else is Hit?”

3 : C
Example 3 But Did It Spread?

- “A classic”: regular desktop starts scanning internally
- Cut from the network soon after: an incident is declared
- An impressive array of malware is discovered; AV is dead
- Problem solved? Did it infect anybody else?!
- Logs from firewalls and flow to the rescue…
Using Logs at Eradication Stage

- Preserving the Log Evidence from Previous Stages
- Confirming that Backups are Safe (Using Logs, How Else?)
- “Is it Gone?"
Example 4 Logs for [Possible] Litigation

- Deliberations on the log retention (and destruction!) policy: IDS, VPN, firewalls, servers – oh, my!
- Decided: IDS – longest; server – next; firewalls, VPN – shortest
- Case: financial information leaked to the media
- Investigation points to a specific user
- Did he do it?!!
- Well, the answer died with 6-mo old VPN logs…
Using Logs at Recovery Stage

- Increased Post- Incident Monitoring
- Watch for Recurrence
- Watch for Related Incidents Elsewhere
- “Better Safe than Sorry”
Example 5 When They Come Back...

- Password guessing hack: non-root account password guessed
- IRC bot, scanning, phishing site setup, etc
- Password changed; attacker files cleaned
- More guessing attempts across the network— are those the same folks?
- *Will they succeed again?*
Using Logs at Follow-Up Stage

- Train Analysts, Responders and Administrators
- Create Management Reports *(Don’t You Love Those! 😊)*
- Verify and Audit Newly Implemented Controls

6: F
Example 6 Logs for Responder Training

- Honeynet #34 Challenge Example
Addendum: Incident Record Keeping

- Retention policy for routine and incident logs
- #1: Human action logs – the longest!
  - Logs created during incident response
- Before planning any log retention policy changes – define incident and routine log retention
- Then: by area, by technology, by business case, etc
  - 2- or 3- Tiered retention strategy is common
So, What Logs are Useful for Incident Response?

- Security Logs vs “Non-Security” Logs
  - Witness confusion in the NIST guide on log management ….

- Let’s quickly go through various logs and see how they help (and helped in specific cases!)
  - Looking at some specifics in the process
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 7 Firewall Logs in Place of Netflow

- Why Look at Firewall Logs During Incident Investigation?
- 1990-2001 – to see what external (inbound) threats got blocked
- 2002-2006 – to see what internal system got connected (out)
- Thus, firewall logs is poor-mans 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] Blocked Attacks
Example 8 Zero-Day Discovery with NIDS

- Can I discover undiscoverable?
- [Mostly] Signature NIDS is still king! But what about those pesky 0days?
- NIDS log pattern discovery to the rescue!
- Samba hack case: 3-4 of the same semi-suspicious signatures firing in the same time sequence => 0day in action
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 😊
Example 9 “Irrelevant, You Say”

- Using disk failures for IDS 😊
- “Detection by catastrophe”
- Is CNN your IDS?
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
Example 10 And What is NOT Stolen?

- Supposedly, all of ChoicePoint 40 mil CCs were not stolen…
- Database logs as a way of non-intrusion detection (or, rather, confirmation)
Proxy Logs in Incident Response

- Internet Access Patterns
- IP theft and/or disclosure
- Policy violations
- Malware: Spyware, Trojans, etc
Client Logs in Incident Response

- FTP client: remote connections and file transfers
- IRC client logs
- Other client software: usually no logs, but usually leave other traces
  - E.g. web browser cache (OK, these are not logs)
Antivirus Logs in Incident Response

- Virus Detection and Clean-up (or lack thereof!)
- Failed and Successful Antivirus Signature Updates
- Other Protection Failures and Issues
- Antivirus Software Crashes and Terminations
“Back to the Process II” 😊

BREAK!!!
Logging Process for IR Review

- Main idea...
  - Log everything
  - Audit little
  - Monitor a bit

- During the incident you'd be grateful you did!
Log Management Process for IR

- Collect the log data
- Convert to a common format
- Reduce in size, if possible
- Transport securely to a central location
- Process in real-time
- Alert on when needed
- Store securely
- Report on trends
Log Management Challenges

- Not enough data
- Too much data
- Diverse records
- Time out of sync
- False records
- Duplicate data
- Hard to get data
- Chain of custody issues
Monitoring or Ignoring Logs Before the Incident?

- How to plan a response strategy to activate when monitoring logs?
- Where to start?
- How to tune it?
Something interesting is seen!

Is it a "known real bad"?

Is this suspicious?

Is it an incident?

Do a preliminary investigation on whether it is an incident

A "false alarm"

Adjust IDS rules that caused a "false alarm"

No action is required!

Start incident response process

Complete the preliminary investigation and take action

Yes

Yes

Yes

Yes

Yes
Value of Logging and Monitoring

Logging
- Audit
- Forensics
- Incident response
- Compliance

Monitoring
- Incident detection
- Loss prevention
- Compliance

Analysis and Mining
- Deeper insight
- Internal attacks
- Fault prediction
“Real-Time” Tasks

- **Malware** outbreaks
- Convincing and reliable **intrusion** evidence
- Serious **internal** network abuse
- **Loss** of **service** on critical assets
Daily Tasks

- Unauthorized configuration changes
- Disruption in other services
- Intrusion evidence
- Suspicious login failures
- Minor malware activity
- Activity summary
Weekly Tasks

- Review inside and perimeter log trends and activities
- Account creation/removal
- Other host and network device changes
- Less critical attack and probe summary
Monthly Tasks

- Review long-term network and perimeter trends
- Minor policy violation summary
- Incident team performance measurements
- Security technology performance measurements
Logs for Incident Response Challenges

- “Can you get’em?” – political boundaries and control issues
- “Can you understand them?” – log format and skill issues
- “Are they kosher?” – logs that can be challenged
Anton’s Five Log Mistakes

How many have you committed? 😊

1. Not looking at logs
2. Not retaining long enough
3. Not normalizing logs
4. Deciding what’s relevant before collection
5. Only looking at known bad
Anton’s Five Incident Response Mistakes

How many have you committed? 😊

1. Not having a plan
2. Failing to increase monitoring and surveillance
3. Being unprepared for a court battle
4. “Putting it back the way it was”
5. Not learning from mistakes
Logs and Laws, Rules, Standards, Frameworks
Laws and Rules that Touch Logs and IR

- HIPAA
- FISMA
- GLBA and SOX (indirectly)
- ISO17799/27001
- COBIT
- Countless others…
Logs in Support of Compliance

- Application and asset risk measurement
- Data collection and storage to satisfy auditing of controls requirements
- Support for security metrics
- Industry best-practices for incident management and reporting
- Proof of security due diligence
### Regulations Recommend Log Management

<table>
<thead>
<tr>
<th>CobiT 4</th>
<th>ISO 17799</th>
<th>NIST 800-53</th>
<th>PCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Provide adequate audit trail for root-cause analysis</td>
<td>- Maintain audit logs for system access and use, changes, faults, corrections, capacity demands</td>
<td>- Capture audit records</td>
<td>- Logging and user activities tracking are critical</td>
</tr>
<tr>
<td>- Use logging and monitoring to detect unusual or abnormal activities</td>
<td>- Review the results of monitoring activities regularly</td>
<td>- Regularly review audit records for unusual activity and violations</td>
<td>- Automate and secure audit trails for event reconstruction</td>
</tr>
<tr>
<td>- Regularly review access, privileges, changes</td>
<td>- Ensure the accuracy of the logs</td>
<td>- Automatically process audit records</td>
<td>- Review logs daily</td>
</tr>
<tr>
<td>- Monitor performance</td>
<td>- Verify backup completion</td>
<td>- Protect audit information from unauthorized deletion</td>
<td>- Retain audit trail history for at least one year</td>
</tr>
<tr>
<td>- Verify backup completion</td>
<td>-</td>
<td>- Retain audit logs</td>
<td>-</td>
</tr>
</tbody>
</table>
Spotlight on: COBIT 4.0

- (Re-)released in Dec 2005
- Four (4) Goals for IT
  - Align IT with business
  - Maximize IT benefits
  - Use IT assets responsibly
  - Manage IT risks
- 34 IT Processes
- Most used framework for SOX compliance
<table>
<thead>
<tr>
<th>Category</th>
<th>Controls</th>
</tr>
</thead>
</table>
| **Identity and Access**| DS5.3  Identity management  
                         | DS5.3  User account management  
                         | PO7.8  Job change and termination                                      |
| **User Activity**      | PO4.11 Segregation of duties  
                         | AI2.3  Application control and audit ability                           |
| **Change**             | AI6.1  Change standards and procedures  
                         | DS9.3  Configuration integrity review                                   |
| **Security**           | DS5.2  IT security plan  
                         | DS5.5  Security testing, surveillance, monitoring  
                         | DS5.10 Network security  
                         | DS11.6  Security requirements for data mgmt                             |
| **IT Infrastructure**  | DS1.5  Monitoring of service level agreements  
                         | DS2.4  Supplier performance monitoring   
                         | DS3.5  Monitoring of performance and capacity   
                         | DS13.3  IT infrastructure monitoring  
                         | DS10.2  Problem tracking and resolution                                  |
| **Business Continuity**| DS4.1  IT continuity framework  
                         | DS4.5  Testing of the IT continuity plan  
                         | DS11.5  Backup and restoration  

Compliance Drives New Controls

Mitigating Risk. Automating Compliance.
From Incident Response to Forensics
Logs and Forensics

- What Makes Your Incident Investigation a “Forensic” Investigation?
- Incident Response vs Forensics
- … and is the ‘vs’ really appropriate?
“Computer forensics is application of the scientific method to digital media in order to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities (Wikipedia)”
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.
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?
What? You think this is evidence? Bua-ha-ha-ha 😊


- **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.”
Example 11 Scan of the Month Challenge #34 Revisited

- Honeypot hacked
- All logs available
- In fact, too many 😊
- Analysis process
Example 12 Sysadmin Gone Bad

- Service Restarts Out of Maintenance Windows
- Correlated with Some Personnel Departures
- Information Leaks Start
- Log Analysis Reveals Unauthorized Software Installation
Example 13 Spyware Galore!

- System Seen Scanning – Firewall Logs
- Analysis of Logs Shows Antivirus Failures
- VPN Logs Help Track the Truth
- Full Forensic Investigation Confirms the Results of Log Analysis
## Example 14 Compromise Detection

<table>
<thead>
<tr>
<th>Security technology/resource</th>
<th>Method</th>
<th>Example</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIDS</td>
<td>Compromise signature</td>
<td>Shell commands on SSL port TCP 443</td>
<td>Medium</td>
</tr>
<tr>
<td>NIDS</td>
<td>Post exploit activity</td>
<td>‘whoami’ in command flow</td>
<td>Medium</td>
</tr>
<tr>
<td>NIDS</td>
<td>Volume of outbound exploits (same or different)</td>
<td>Lots of SSL hits out</td>
<td>Medium</td>
</tr>
<tr>
<td>NIDS</td>
<td>Volume of outbound exploits after a similar inbound exploit</td>
<td>Lots of SSL hits out after the system is hit by SSL exploit</td>
<td>High</td>
</tr>
<tr>
<td>NIDS, firewall</td>
<td>Outbound massive port scanning, DoS, etc</td>
<td>Many connections to port 1434 UDP from a single system</td>
<td>Medium</td>
</tr>
<tr>
<td>HIDS</td>
<td>Abuse-related system log records</td>
<td>New account created</td>
<td>Medium</td>
</tr>
<tr>
<td>HIPS</td>
<td>Application behaving significantly different from known good</td>
<td>Connections, registry access, file replacements</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Conclusion

- Turn ON Logging!!!
- Make Sure Logs Are There When You Need Them (and need them you will 😊)
- Include Log Analysis into the IH Process
- Avoid Above (and Other) Mistakes
- Prepare and Learn the Analysis Tools
- When Going Into the Incident-Induced Panic Think ‘It's All Logged Somewhere – We Just Need to Dig it Out’ 😊
Anton Chuvakin, Ph.D., GCIA, GCIH, GCFA
anton@chuvakin.org
Director of Security Research
LogLogic, Inc


Contributor to “Hacker’s Challenge 3” (Osborne 2006)

**Book on logs is coming soon!**

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