



Guy Bruneau, GSE

LOG, LOG, LOG EVERYTHING REMOTELY

About Me

- Senior Security Consultant @ipss inc.
- Incident Handler @Internet Storm Center
 - gbruneau@isc.sans.edu
- SIEM user since 2001, IDS before that
- Mid to large enterprises
-  @GuyBruneau

Agenda

- ⦿ Why collect logs and/or packets?
- ⦿ How much can I trust my equipment?
- ⦿ Collection, detection and reporting
- ⦿ Some logging devices
 - Open Source (free)
 - Commercial



Network Forensics – What & Why?

- ⦿ Defined as analysis of network traffic or network events
- ⦿ Accuracy requires collecting everything, well almost
- ⦿ Without accurate logs, incident response is difficult
- ⦿ Almost impossible to assess real impact
- ⦿ Packet collection enhances incident resolution



How Good Is My Equipment?

- ◎ NSS Labs testing shows 98.5% effectiveness
 - IPS, NGFW, endpoint protection system
 - 1.5% bypass perimeter and host layer defenses
 - Stealthy attacks give control to malicious actors
- ◎ Suggest: Control the attacker by redirecting the attack against a target you can watch and control
- ◎ Reality: Catch what you can detect and block
- ◎ Are you prepared to operate at 60% capacity?
 - Withstand a breach, with reduced services
 - Example: Home Depot, JP Morgan Chase

Collect & Centralize Logs - Challenges

- ⦿ Voluminous amount of logs to process
 - 100 events per second is >8 billion events/day
- ⦿ Managing system logs into meaningful intelligence
 - Can you find that needle in the haystack?
- ⦿ High speed networks are challenging packet collection and metadata accuracy
- ⦿ Accurate packet collection is dependant on speed and storage capacity
- ⦿ How complete and accurate is the data?

Regulations - Failure

- ⦿ Failure to comply can have painful results
 - Fines/penalties
 - Additional audits
 - Loss of brand value
 - Delay/hard stop on business processes
- ⦿ Exposures may result
 - Customer and investigation costs
 - Loss of customers
 - Lawsuits

End Goals

- ① Centralize logging
- ① Consider event rate
- ① Normalize the data (system independent)
- ① Reporting and analysis functions
- ① Notification and alerting
- ① Minimum administration

Password Guessing – SQL Attack

- Would you want to know someone is after your SQL database?

```
Logon Type: 10
Account For Which Logon Failed:
  Security ID: NULL SID
  Account Name: root
  Account Domain: DBSERVER
Failure Information:
  Failure Reason: Unknown user name or bad password.
  Status: 0xc000006d
  Sub Status: 0xc0000064
```

```
Logon Type: 10
Account For Which Logon Failed:
  Security ID: NULL SID
  Account Name: kelly
  Account Domain: DBSERVER
Failure Information:
  Failure Reason: Unknown user name or bad password.
  Status: 0xc000006d
  Sub Status: 0xc0000064
```

```
Logon Type: 10
Account For Which Logon Failed:
  Security ID: NULL SID
  Account Name: sql
  Account Domain: DBSERVER
Failure Information:
  Failure Reason: Unknown user name or bad password.
  Status: 0xc000006d
  Sub Status: 0xc0000064
```

Free Loggers

- ⦿ Basic syslog server
- ⦿ Sagan → Sguil Database
- ⦿ Windows Syslog Server
- ⦿ NXLOG Community Edition
 - Supports Unix, Android, Windows, etc
 - Read logs from various databases

<http://nxlog-ce.sourceforge.net>
<http://log4ensics.com/features>

Basic Syslog Server

The screenshot shows the Syslog Server 1.2.0 application window. The title bar reads "Syslog Server 1.2.0". The menu bar includes "App", "View", "Action", "Settings", "Macros", and "Help".

The main area is titled "SysLog (View by Severity)" and contains a legend for severity levels:

- Emergency: system is unusable
- Alert: action must be taken immediately
- Critical: Critical conditions
- Error: Error conditions
- Warning: Warning conditions
- Notice: normal but significant condition
- Informational: Informational messages
- Debug: debug-level messages

Below the legend is an "Events" table with the following data:

EventIdx	Facility	Severity	Message	TimeStamp
991	5	4	klogd: DROP IN=vlan2 OUT= MAC=ff:ff:ff:ff:00:1b:d5:fe:e7:dd:08:00	12/2/2012 12:34:46 PM
990	5	4	klogd: DROP IN=vlan2 OUT= MAC=ff:ff:ff:ff:00:1b:d5:fe:e7:dd:08:00	12/2/2012 12:34:44 PM
989	5	4	klogd: REJECT v6: calling icmpv6_send	12/2/2012 12:34:37 PM
986	5	4	klogd: REJECT v6: calling icmpv6_send	12/2/2012 12:34:30 PM
983	5	4	klogd: REJECT v6: calling icmpv6_send	12/2/2012 12:34:26 PM
980	5	4	klogd: DROP IN=vlan2 OUT= MAC=ff:ff:ff:ff:00:1b:d5:fe:e7:dd:08:00	12/2/2012 12:34:23 PM
979	5	4	klogd: DROP IN=vlan2 OUT= MAC=ff:ff:ff:ff:00:1b:d5:fe:e7:dd:08:00	12/2/2012 12:34:21 PM

Below the table is an "Event detail" section with input fields for "Event ID", "TimeStamp", "Host name", "Host IP", "Facility", and "Severity".

At the bottom of the window, a status bar displays the following text: "[DATA] from 192.168.25.1 -- <44>klogd: DROP IN=vlan2 OUT= MAC=ff:ff:ff:ff:00:1b:d5:fe:e7:dd:08:00 SRC=10.125.246.1 DST=25".

Sagan → Sguil Database

Dashboard Events Welcome [guy](#) | [Logout](#) [comments](#) [sensors](#) [filters](#)

< 2012 Jan Feb Mar Apr May Jun Jul Aug Sep Oct **Nov** Dec 2014 >

Timeline: 2013-11-15 00:00:00 until 2013-11-15 23:59:59 (+00:00) Filtered by Object: NO Filtered by Sensor: NO Status: [Synchronized](#)

Toggle

Event Grouping: on

Event Queue Only: on

Map: off

Event Summary

Queued Events: 211

Total Events: 49142

Total Signatures: 15

Total Sources: -

Total Destinations: -

Event Count by Priority

High: 207 (98.1%)

Medium: -

Low: 4 (1.9%)

Other: -

Event Count by Classification

- Admin Access: -
- User Access: -
- Attempted Access: -
- Denial of Service: -
- Policy Violation: -
- Reconnaissance: -
- Malware: -

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
98.1%								
4	4	1		23:16:57	[OPENSSSH] No identification string - possible scan	5000070	6	0.008%
18	1	1		11:56:10	[OPENSSSH] Invalid or illegal user [oracle]	5001113	6	0.037%
20	1	1		11:55:33	[OPENSSSH] Invalid or illegal user [guest]	5001109	6	0.041%
26	1	1		11:54:31	[OPENSSSH] Invalid or illegal user [admin]	5001107	6	0.053%
19	1	1		11:54:26	[OPENSSSH] Invalid or illegal user [webmaster]	5001118	6	0.039%
25	1	1		11:54:16	[OPENSSSH] Invalid or illegal user [test]	5001115	6	0.051%
17	1	1		11:54:15	[OPENSSSH] Invalid or illegal user [postgres]	5001114	6	0.035%
15	1	1		11:53:36	[OPENSSSH] Invalid or illegal user [info]	5001110	6	0.031%
12	1	1		11:52:52	[OPENSSSH] Invalid or illegal user [web]	5001117	6	0.024%
15	1	1		11:11:43	[OPENSSSH] Invalid or illegal user [user]	5001116	6	0.031%
2	1	1		11:06:44	[OPENSSSH] Attempt to login using a denied user	5000077	6	0.004%
6	1	1		10:57:29	[OPENSSSH] Invalid or illegal user [nagios]	5001112	6	0.012%
20	3	1		10:20:02	[OPENSSSH] Invalid or illegal user	5000022	6	0.041%
4	2	1		10:20:02	[OPENSSSH] Invalid or illegal user [a]	5001106	6	0.008%
8	1	1		10:20:02	[OPENSSSH] Failed password - Brute force	5001646	6	0.016%

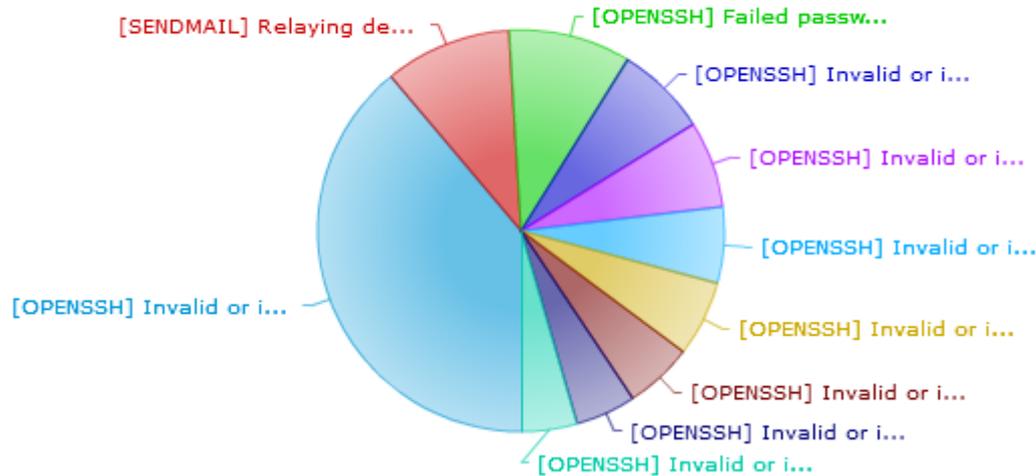
update

Commercial Products

- ⦿ Evaluations available
 - HP ArcSight
 - Splunk
- ⦿ IBM QRadar
- ⦿ RSA Security Analytics → Log Decoder
- ⦿ Snare → Sends Windows logs in syslog format

ArcSight Logger – Unix Logs

Top 10 Events



- [OPENSSH] Invalid or illegal user
- [SENDMAIL] Relaying denied [reject=550 5.7.1]
- [OPENSSH] Failed password - Brute force
- [OPENSSH] Invalid or illegal user [test]
- [OPENSSH] Invalid or illegal user [oracle]
- [OPENSSH] Invalid or illegal user [guest]
- [OPENSSH] Invalid or illegal user [admin]
- [OPENSSH] Invalid or illegal user [postgres]
- [OPENSSH] Invalid or illegal user [nagios]
- [OPENSSH] Invalid or illegal user [info]

deviceEventClassId	_count
[OPENSSH] Invalid or illegal user	324
[SENDMAIL] Relaying denied [reject=550 5.7.1]	84
[OPENSSH] Failed password - Brute force	81
[OPENSSH] Invalid or illegal user [test]	61
[OPENSSH] Invalid or illegal user [oracle]	58
[OPENSSH] Invalid or illegal user [guest]	51
[OPENSSH] Invalid or illegal user [admin]	51

Summary

- ⦿ Inaccurate (or absent) logs = difficult incident response
- ⦿ Meeting regulations more than just a check box (PCI, PEPIDA)
- ⦿ Can you survive a breach?
 - Operate at 60%, contain and investigate

