OWASP Logging Guide

SUMMARY

Why log ?

- identify security incidents
- monitor policy violations
- identify fraudulent activity
- identify operational and longterm problems
- establish baselines
- ensure compliance with laws,rules and regulations

What is commonly logged ?

NB Much of the info below can only be logged by the applications themselves (this is especially true for applications used through encrypted network communications)

- Client requests and server responses
- Account activities (login, logout, change password etc.)
- Usage information (transaction types and sizes, generated traffic etc.)
- Significant operational actions such as application startup and shutdown, application failures, and major application configuration changes. This can be used to identify security compromises and operational failures.

What are security logs ?

- security software logs (Antimalware Software, IDS, IPS, Remote Access Software, Web Proxies, Vulnerability Management Software, Authentication Servers, Routers, Firewalls)
- operating system logs (System Events, Audit Records)
- application and database logs
  - commercial offtheshelf (COTS) applications (s.a . email servers and clients, Web servers and browsers, file servers and file sharing clients, database servers and clients, ERP and CRM systems)
  - **custom-developed applications**

What are the most common issues with logging ?

- high number of log sources
- inconsistent log content
- inconsistent log formats
- inconsistent timestamps
- increasingly large volumes of log data

What are the common functions of a log management infrastructure ?

General

- Log parsing
- Event filtering (e.g. suppression of duplicate entries and standard informational entries)
- Event aggregation (see Figure 1 - OSSIM correlation)

Storage

- Log rotation
- Log archival
- Log compression
- Log reduction
- Log conversion
- Log normalization (e.g. storing dates and times in a single format)
- Log file integrity checking (involves calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected).

Analysis

- Event correlation
  - rulebased correlation
  - using statistical methods or visualization tools

  See Figure 2 – OSSIM example – alerts resulting from correlation
- Log viewing (displaying log entries in a human-readable format)
- Log reporting is displaying the results of log analysis. Log reporting is often performed to summarize significant activity over a particular period of time or to record detailed information related to a particular event or series of events.

Disposal

How to plan a logging infrastructure ?

- develop standard processes for log management
- define its logging requirements and goals
- define mandatory requirements and suggested recommendations for log management activities
- prioritize the requirements/goals based on the organization’s perceived reduction of risk and the expected time and resources needed to perform log management functions
- prioritize/classify data in order to log/analyze data that is of greatest importance

  (e.g. Business data, Application binaries, configurations and documentation, System binaries, configurations and documentation, Application and database logs, System logs.
  For each data class, criteria such as criticality, security and retention duration requirements must be defined.
- define roles and responsibilities for log management for key personnel throughout the organization, including log management duties at both the individual system level and the log management infrastructure level
- create and maintain a log management infrastructure
- define standard log management operational processes (configuring log sources, performing log analysis, initiating responses to identified events, managing longterm storage, monitoring the logging status of all log sources, monitoring log rotation and archival, checking for upgrades and patches to logging software, and acquiring, testing, and deploying them, ensuring that each logging host’s clock is synched to a common time source, reconfiguring logging as needed based on policy changes, technology changes, and other factors, documenting and reporting anomalies in log settings, configurations, and processes).

(Source : http://csrc.nist.gov/publications/nistpubs/80092/SP80092.pdf)

What is log management ?

- log generation
- transmission
- storage
- analysis
- disposal
- ensuring that security, system, and network administrators regularly perform effective analysis of log data
- protecting the confidentiality, integrity, and availability of logs

What application logs/events to monitor ?

What to monitor ?	**Pros**	**Cons**
SQL statements generated by application activity	Easier to baseline than SQL issued by DBAs, developers and power users	High volume
Sequence monitoring (base on multiple activities) : (pattern of activity, frequence of activity, order between activities)	This gives us a window of opportunity to block an attack	Difficult to implement/configure
What data is returned on which session ? ; How much data is returned ?	Can help us identify compromised sessions/accounts	Difficult to implement/configure
monitor usage of procedures and packages that are vulnerable and/or useful in attacks ; profile under what conditions they are used normally Example : white list of users and white list of IPs for the use of UTL_SMTP Example : black list of errors that we do not allow for any session An “unknown column” error might indicate an SQL injection attack	Can allow us to quickly identify attacks and terminate rogue sessions	This measure is less reliable than implementing reactive session termination in the application (e.g. a session provoking s.a. errors gets terminated by the application)
A single user credential that is concurrently being used from different IPs is at least a misuse of credentials and sometimes an intrusion	Can allow us to fight against misuse of credentials and intrusions	Not always possible : Centralized session management is a prerequisite
Events related to known application vulnerabilities that have not yet been addressed	Can represent a quick protection against such vulnerabilities in the application.	Temporary solution. Can be used as an excuse to delay implementation of proper defenses in the application

To be continued/detailed…

Application logs and Security Information Management systems

Case study - OSSIM (Open Source Security Information Management system)

Ossim's generic correlation engine allows us to configure alerts based on information from:

- the integrated software components detailed below
- various provided plugins (WMWare Workstation, OpteNEt, Nepenthes, ISA Server, Aladdin, Avast, Bro-IDS, Enterasys Dragon, Honeyd, MCAfee Antivirus, Sidewinder, SonicWall, Trendmicro, Cyberguard, VSftpd, Bind etc.)
- **application logs**

  *** In order to generate IDS events/alerts from your customs-developed applications' logs :

  the logs must be consistent (content, format, timestamps) ;

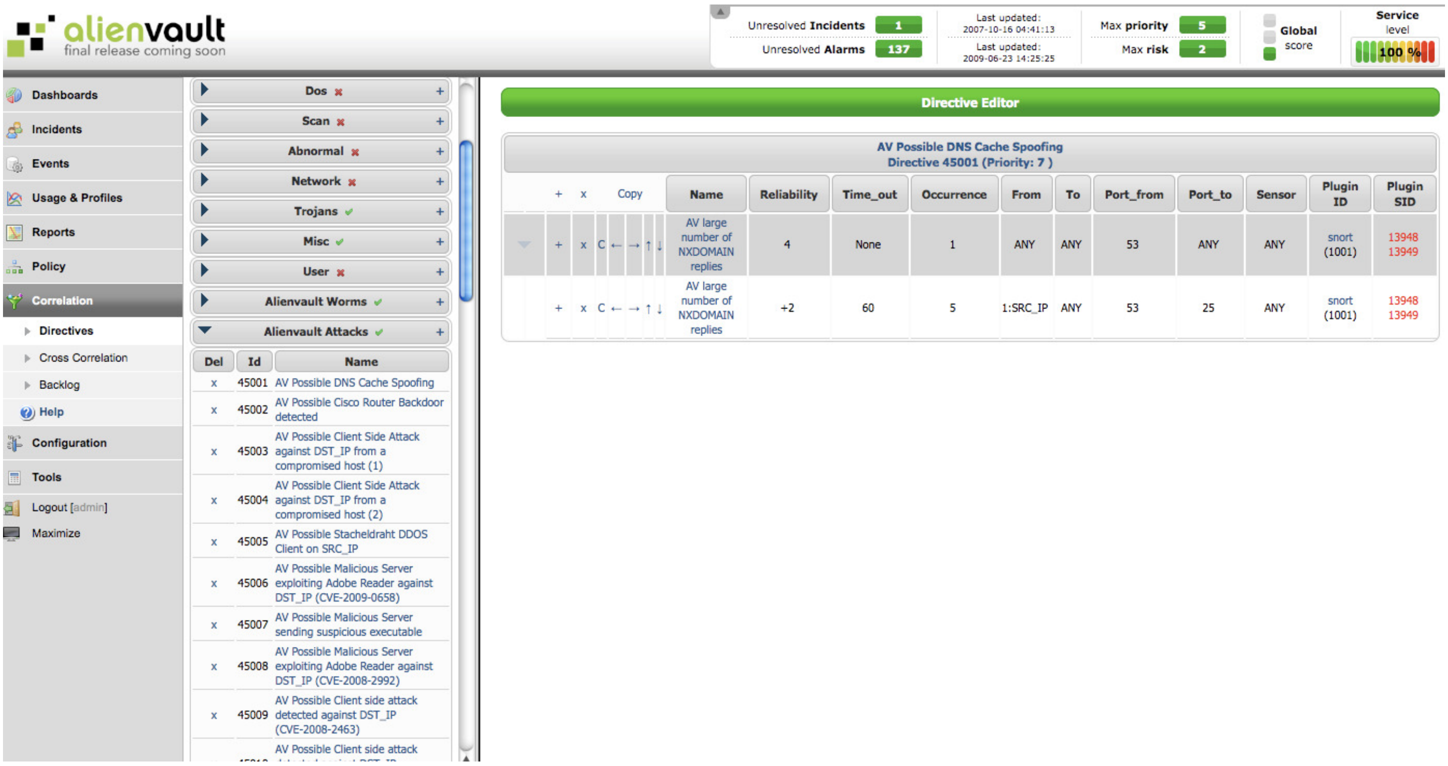
  you need to write your own OSSIM plugin (no need to be scared, plugin writing amounts to finding the right regular expression)

Ossim software components

* Arpwatch, used for mac anomaly detection.
* P0f, used for passive OS detection and os change analisys.
* Pads, used for service anomaly detection.
* Nessus/OpenVAS, used for vulnerability assessment and for cross correlation (IDS vs Security Scanner).
* Snort, the IDS, also used for cross correlation with nessus.
* Spade, the statistical packet anomaly detection engine. Used to gain knowledge about attacks without signature.
* Tcptrack, used for session data information which can grant useful information for attack correlation.
* Ntop, which builds an impressive network information database from which we can get aberrant behaviour anomaly detection.
* Nagios. Being fed from the host asset database it monitors host and service availability information.
* Osiris, a great HIDS.
* OCS-NG, Cross-Platform inventory solution.
* OSSEC, integrity, rootkit, registry detection and more.

Figure 1 - OSSIM correlation. The Directive Editor allows us to define what events to correlate.

The number of occurrences for each event is used to calculate reliability (see Event aggregation)



Unresolved **Incidents** 1
Unresolved **Alarms** 137

Last updated: 2007-10-16 04:41:13
Last updated: 2009-06-23 14:25:25

Max **priority** 5
Max **risk** 2

Global score

Service level 100 %

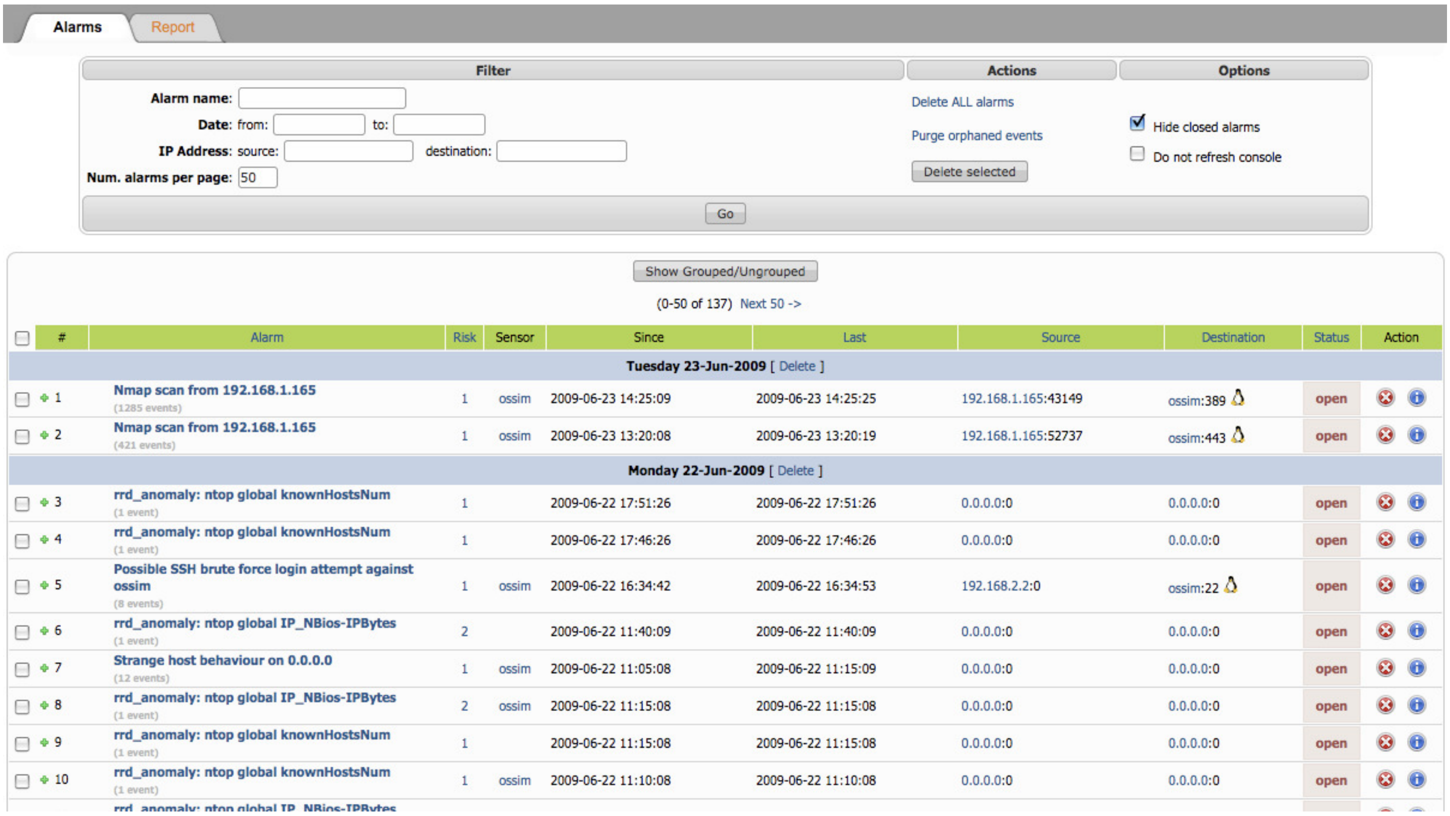
Del	Id	Name
x	45001	AV Possible DNS Cache Spoofing
x	45002	AV Possible Cisco Router Backdoor detected
x	45003	AV Possible Client Side Attack against DST_IP from a compromised host (1)
x	45004	AV Possible Client Side Attack against DST_IP from a compromised host (2)
x	45005	AV Possible Stacheldraht DDOS Client on SRC_IP
x	45006	AV Possible Malicious Server exploiting Adobe Reader against DST_IP (CVE-2009-0658)
x	45007	AV Possible Malicious Server sending suspicious executable
x	45008	AV Possible Malicious Server exploiting Adobe Reader against DST_IP (CVE-2008-2992)
x	45009	AV Possible Client side attack detected against DST_IP (CVE-2008-2463)
		AV Possible Client side attack

Directive Editor

AV Possible DNS Cache Spoofing
Directive 45001 (Priority: 7)

+	x	Copy	Name	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Sensor	Plugin ID	Plugin SID
+	x	C ← → ↑ ↓	AV large number of NXDOMAIN replies	4	None	1	ANY	ANY	53	ANY	ANY	snort (1001)	13948 13949
+	x	C ← → ↑ ↓	AV large number of NXDOMAIN replies	+2	60	5	1:SRC_IP	ANY	53	25	ANY	snort (1001)	13948 13949

Figure 2 - OSSIM example. Alerts resulting from correlation.



Filter	Actions	Options
Alarm name:	Delete ALL alarms	☑ Hide closed alarms
Date: from: to:	Purge orphaned events	□ Do not refresh console
IP Address: source: destination:	Delete selected	
Num. alarms per page: 50		

(0-50 of 137) Next 50 ->

□	#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
		Tuesday 23-Jun-2009 [Delete]								
□	+ 1	**Nmap scan from 192.168.1.165** (1285 events)	1	ossim	2009-06-23 14:25:09	2009-06-23 14:25:25	192.168.1.165:43149	ossim:389	open	
□	+ 2	**Nmap scan from 192.168.1.165** (421 events)	1	ossim	2009-06-23 13:20:08	2009-06-23 13:20:19	192.168.1.165:52737	ossim:443	open	
		Monday 22-Jun-2009 [Delete]								
□	+ 3	**rrd_anomaly: ntop global knownHostsNum** (1 event)	1		2009-06-22 17:51:26	2009-06-22 17:51:26	0.0.0.0:0	0.0.0.0:0	open	
□	+ 4	**rrd_anomaly: ntop global knownHostsNum** (1 event)	1		2009-06-22 17:46:26	2009-06-22 17:46:26	0.0.0.0:0	0.0.0.0:0	open	
□	+ 5	**Possible SSH brute force login attempt against ossim** (8 events)	1	ossim	2009-06-22 16:34:42	2009-06-22 16:34:53	192.168.2.2:0	ossim:22	open	
□	+ 6	**rrd_anomaly: ntop global IP_NBios-IPBytes** (1 event)	2		2009-06-22 11:40:09	2009-06-22 11:40:09	0.0.0.0:0	0.0.0.0:0	open	
□	+ 7	**Strange host behaviour on 0.0.0.0** (12 events)	1	ossim	2009-06-22 11:05:08	2009-06-22 11:15:09	0.0.0.0:0	0.0.0.0:0	open	
□	+ 8	**rrd_anomaly: ntop global IP_NBios-IPBytes** (1 event)	2	ossim	2009-06-22 11:15:08	2009-06-22 11:15:08	0.0.0.0:0	0.0.0.0:0	open	
□	+ 9	**rrd_anomaly: ntop global knownHostsNum** (1 event)	1		2009-06-22 11:15:08	2009-06-22 11:15:08	0.0.0.0:0	0.0.0.0:0	open	
□	+ 10	**rrd_anomaly: ntop global knownHostsNum** (1 event)	1	ossim	2009-06-22 11:10:08	2009-06-22 11:10:08	0.0.0.0:0	0.0.0.0:0	open	
		rrd_anomaly: ntop global IP_NBios-IPBytes								

Tools

Tool	Role	Link
Splunk	indexes all of your IT data in real time, without requiring you to write connectors, plugins, custom parsers or controls	http://www.splunk.com
Ossim	Open Source Security Information Management system	https://www.ossim.net/

References

http://csrc.nist.gov/publications/nistpubs/80092/SP80092.pdf

https://www.ossim.net/

http://www.splunk.com/base/Documentation/latest/User/SplunkOverview