Week 9: Logging and Forensics

Logging

NIST provide a formal definition of what is a log:
“A log is a record of the events occurring within an organization’s systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network."(Kent & Souppaya, 2006)

Many applications and servers such as web servers, database servers produce logs. There are also softwares designed to analyse logs. log messages mostly consist of the following fields; time, hostname, program name and status.

History

Syslog was part of the system logging on the BSD operating system. It was later formalised as a standard for logging leading to the RFC 5424.

Most Unix systems keep their logs in the var/log directory. These files are text-based files that can be read by a standard text reader.

Logs are grouped into various sets as detailed below;

- Var/log/syslog or var/log/messages: holds all the system level messages
- /var/log/auth.log and /var/log/secure both keep a history of logins and authentications (both successful and failed attempts)
- /var/log/boot.log: keeps a history of boot-up messages
- /var/log/maillog or /var/log/mail.log: keeps a history of messages from whatever mail servers are running on the system.
- /var/log/kern: contain a history of kernel generated messages
- /var/log/dmesg
- and other logs: web servers (usually /var/log/httpd) databases (e.g. /var/log/mysqld.log) and ftp servers (var/log/ftp.log) amongst many others

logrotate is a key log management utility used to manage the number of instances of each log to keep, when to create a new log file, when and how to archive old logs, and even whether to email logs to another destination. The many varied configuration options are kept in a /etc/logrotate.conf file. Detailed information about the logrotate command as always can be obtained via the standard Unix MAN command.

On Windows system, event viewer is used to access logs.

Log entries are classified by types such as error, information, warning, success audit and failure audit (for windows systems), emergency, alert, critical, error, warning, notice, info, debug (for MacOS and Linux systems)

Logs can be stored locally or remotely or both. A compromised machine might have its logs deleted by attacker or even impossible to access therefore It is imperative to be able to access logs from other locations. Logs can also be written to multiple machines if required.

Logging Tools

Syslog-ng

The main benefits are:

- The default use of TCP links.
- Better filtering.
- More comprehensive routing options via templates.
- More accurate timestamps.

It is available as an open-source (LGPL version) and as a commercial supported version. It is available either as an option or as standard in several GNU/Linux distributions.

Nagios

Nagios is an open-source log-aggregation and monitoring tool. It is usually hosted on a Linux server. It can also monitor hardware and network infrastructure via a large selection of agents and plug-ins. It can even use SNMP (simple network management protocol) to gather data from even the most basic appliances. It can write log data to various database servers and display data as web pages or text alerts.

Snort

It is as an open-source intrusion detection/ prevention system. It can run in either of these three modes. Sniffer, Logger, Network Intrusion Detection System. It is often with in combination with other analysis tools to create a SIEM (Security Information and Event Management)-like solution.

Computer Security Breaches

Attacks are currently on the rise and getting more sophisticated. The damage to a business can be brutal. The only way to survive these attacks is to have a tested and trusted business continuity plan which should be done in accordance with IS0 22301. An effective plan must follow the PDCA (Plan, Do, Check, Act) mandate.

Breach Response Checklist

Once a breach has been detected, the following steps should be carried out according to Irwin (2009):

1) Check what types of data were affected?
2) Determine what happened? (how)
3) Determine who was responsible?
4) Stop any escalation(s)
5) Instigate Business Continuity Plan
6) Determine whether the ICO needs to be notified
7) Determine whether affected individuals need to be notified

“Digital Forensics, also referred to as computer forensics is a specialisation within the industry that converges with traditional forensic science. It is concerned with the recovery of digital evidence from storage media, computer systems, electronic devices and social media platforms” (Campbell, 2016).

Forensic Process from NIST SP-800-86

Collection -> Examination -> Analysis -> Reporting

Forensic tools

When choosing forensic tools, one must ensure that all eventualities are covered by the choice of tool. Eventualities include:

- Breach delivered as an email payload, launched when the user opens the mail or clicks on a link.
- A worm delivered on the internet
- A disgruntled employee
- Exploiting a vulnerability in some system component

A full forensic investigation requires that the investigation team evaluates every part of the system.

1) Examining the RAM and storage areas of the disk
2) Scanning storage media looking for emails or zip files that may have contained a payload
3) Existing applications need to be checked to ensure that they haven’t been replaced by malware
4) Existing systems should be scanned and checked to ensure all components are patched up to date and there are no obvious security vulnerabilities
5) Logs should be copied and examined looking for evidence of how and when the breach occurred.