Variations of logs

When you purchase an item in a store, you usually receive a receipt as a record of purchase.
The receipt breaks down the transaction information with details such as the date and time, the cashier's name, the item name, cost, and the method of payment.
But, not all store receipts look the same.
For example, receipts like automotive invoices use lots of detail when listing the items or services that were sold.
You most likely won't find this much detail from a restaurant receipt.
Despite the differences among store receipts, all receipts contain important details that are relevant to the transaction.
Logs are similar to receipts.
While receipts record purchases, logs record the events or activities that happen on a network or system.
As a security analyst, you'll be responsible for interpreting logs.
Logs come in different formats, so not all logs look the same.
But, they usually contain information like timestamps, system characteristics, like IP addresses, and a description of the event, including the action taken and who performed the action.
We know that logs can be generated from many different data sources such as network devices, operating systems, and more.
These log sources generate logs in different formats.
Some log formats are designed to be human-readable while others are machine-readable.
Some logs can be verbose, which means they contain lots of information, while some are short and simple.
Let's explore some commonly used log formats.
One of the most commonly used log formats is Syslog.
Syslog is both a protocol and a log format.
As a protocol, it transports and writes logs.
As a log format, it contains a header, followed by structured-data, and a message.
The Syslog entry includes three sections: a header, structured-data, and a message.
The header contains data fields like Timestamp, the Hostname, the Application name, and the Message ID.
The structured-data portion contains additional data information in key-value pairs.
Here, the eventSource is a key that specifies the data source of the log, which is the value Application.
Lastly, the message component contains the detailed log message about the event.
In this example, "This is a log entry!" is the message.
Let's explore another common log format you might encounter as a security analyst.
JavaScript Object Notation, more popularly known as JSON, is a text-based format designed to be easy to read and write.
It also uses key-value pairs to structure data.
Here's an example of a JSON log.
The curly brackets represent the beginning and end of an object.

The object is the data that's enclosed between the brackets.
It's organized using key-value pairs where each key has a corresponding value separated by colons.
For example, for the first line, the key is Alert and the value is Malware.
JSON is known for its simplicity and easy readability.
As a security analyst, you'll use JSON to read and write data like logs.
eXtensible Markup Language, or XML, is a language and a format used for storing and transmitting data.
Instead of key-value pairs, it uses tags and other keys to structure data.
Here, we have an example of an XML log entry with four fields: firstName, lastName, employeeID, and dateJoined, which are separated with arrows.
Finally, Comma Separated Values, or CSV, is a format that uses separators like commas to separate data values.
In this example, there are many different data fields which are separated with commas.
Now that you know about the diversity of log formats, you can focus on evaluating logs to build context around a detection.
Coming up, you'll explore how IDS signatures are used to detect, log, and alert on suspicious activity.

Revision #1
Created 2 November 2023 07:24:40 by naruzkurai
Updated 2 November 2023 07:24:57 by naruzkurai