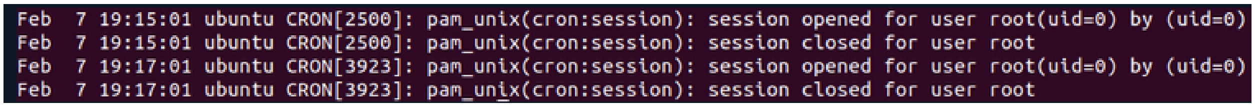
Log Collection Analysis & Review

By: Ryan Stewart

SIEM Log Collection Process Overview

In the realm of Security Information and Event Management (SIEM), the log collection process is paramount for threat detection. Logs, which record events and messages in a system, serve as the lifeblood of SIEM. Without a robust log collection system, SIEM's effectiveness diminishes.



```
Feb  7 19:15:01 ubuntu CRON[2500]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Feb  7 19:15:01 ubuntu CRON[2500]: pam_unix(cron:session): session closed for user root
Feb  7 19:17:01 ubuntu CRON[3923]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Feb  7 19:17:01 ubuntu CRON[3923]: pam_unix(cron:session): session closed for user root
```

What is Log and Logging?

In computing, a log file captures events in an operating system or other software runs, serving as a record of communication between users. Logging is the practice of keeping such records. Typically, a log includes basic information like time, source system, and a message.

For instance, inspecting "/var/log/auth.log" on an Ubuntu server reveals source, time, and message information. Our goal at this point is to transfer logs from various places (**Hosts, Firewall, Server log, Proxy, etc.**) to SIEM. Thus, we can process all data and detect threats at a central point. Logs are generally collected in the following 2 ways:

Log Collection Methods

Logs are gathered through two primary methods: **Log Agents and Agentless.**

Log Agents

Log Agents involve employing specialized software agents. These agents often offer parsing, log rotation, buffering, log integrity, encryption, and conversion features. While efficient, activating additional features increases resource consumption, impacting CPU and RAM.

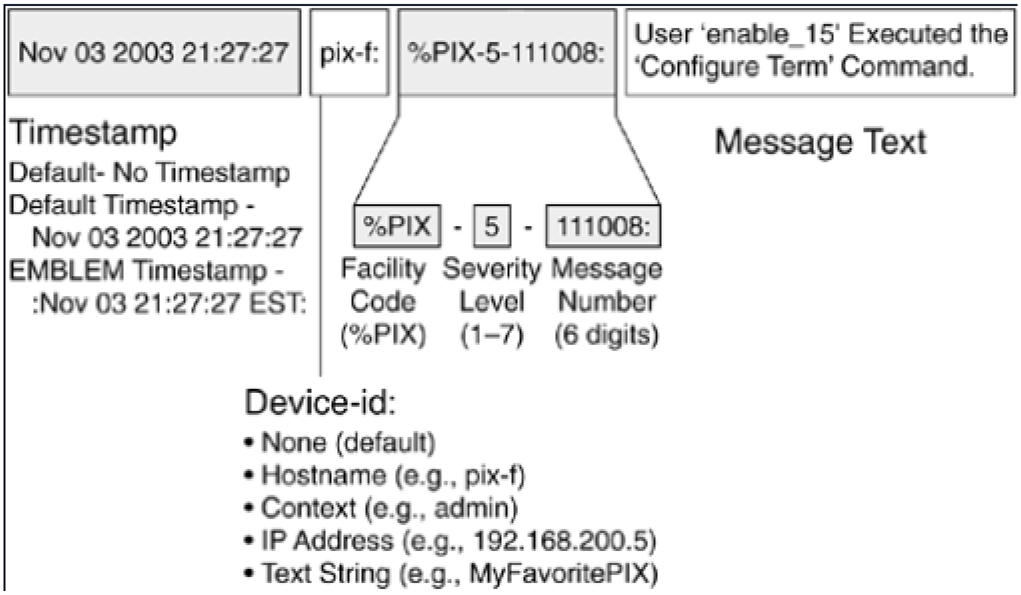
Pros:
- Tested and proven by developers.
- Offers advanced features like automatic parsing and encryption.

Cons:
- Increased resource consumption and associated costs.

Syslog

Syslog, a widely used network protocol, supports log transfers over UDP or TCP and optional TLS encryption. Devices like switches, routers, IDS, firewalls, and various operating systems can leverage syslog. Log agents can transfer logs using Syslog by parsing them into the **syslog format.**

Syslog Format:
Timestamp - Source Device - Facility - Severity - Message Number - Message Text



```
Nov 03 2003 21:27:27 pix-f: %PIX-5-111008: User ‘enable_15’ Executed the ‘Configure Term’ Command.
```

Note:

- **Maximum packet size for Syslog** UDP is 1024 bytes, while for TCP, it's 4096 bytes.

3rd Party Agents

Many SIEM products offer their own agent software. Examples include:
- Splunk: universal forwarder
- ArcSight: ArcSight Connectors

These agents integrate seamlessly with SIEM, providing advanced parsing capabilities.

Popular Open Source Agents:
- Beats: [elastic.co/beats](https://www.elastic.co/beats/)
- NXLog: nxlog.co

Agentless

Agentless log sending involves connecting to the target system through protocols like SSH or WMI. It is cost-effective, but poses a security risk due to the need for username and password credentials. It is easier to set up and manage than the agent method but comes with limited capabilities.

Manual Collection

In situations where existing agents fall short, manual collection involves writing custom scripts. This approach is necessary, for instance, when dealing with logs from a cloud-based application that cannot be read by existing agents.

Summary

The diversity in log collection methods, ranging from agents to agentless, allows for flexibility in various scenarios. When off-the-shelf agents prove insufficient, the ability to craft custom scripts ensures comprehensive log coverage for effective SIEM utilization.

Quiz Questions:

1. What is the preferred method for those averse to managing agent software?
   - A) Log Agents
   - B) Agentless
   - C) Syslog
   - D) 3rd Party Agents

2. Universal Forwarder is the agent software associated with which product?
   - A) Splunk
   - B) ArcSight
   - C) NXLog
   - D) Beats