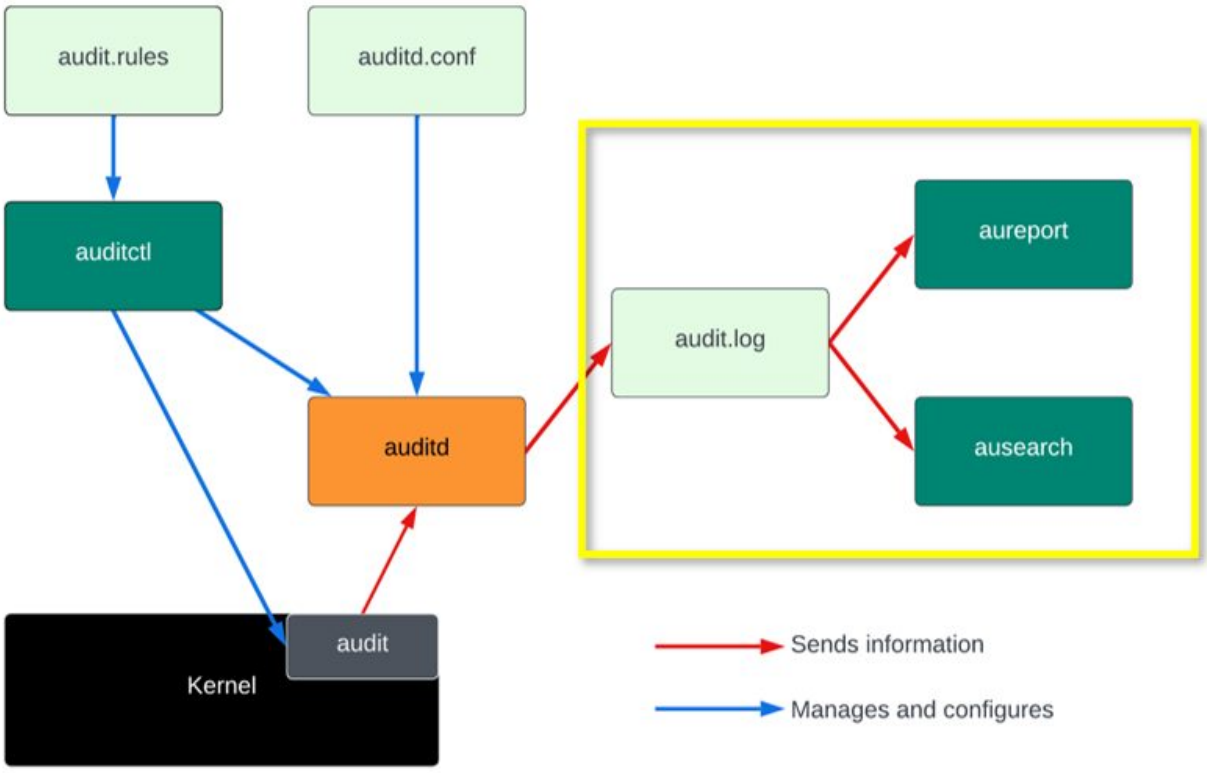
Linux Incident Response - Understanding Auditd

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-09

Overview

Auditd is the userspace component of the Linux Auditing System, an in-built feature of the Linux kernel that allows systems administrators to monitor and track security-relevant information, ensuring system integrity and compliance with various regulations. It is designed to integrate with SELinux (Security-Enhanced Linux), which enforces security policies including mandatory access controls (MAC). When certain system calls are invoked, auditd logs this activity according to rules defined by the administrator, providing a reliable trail that can be inspected in the event of a security incident.



Simplified view of how the auditing components relate to each other

The audit daemon is configured via the auditd.conf file, typically located at /etc/audit/auditd.conf. This configuration file allows the administrator to set parameters such as the maximum size of the log file, the action to take when the log is full (e.g., rotate the log or halt the system), and the location of the log file. Administrators can also define the rate at which messages are sent to the audit log to prevent flooding the system with monitoring messages, which could potentially impact performance.

Auditd collects data by hooking into the Linux kernel audit framework, which intercepts system calls and generates audit records. These records are then passed to auditd, which processes them and writes them to the audit log. The data captured includes system calls made by users and processes, manipulations of files and directories, and changes to user accounts and group memberships. This breadth of captured data makes auditd a powerful tool for monitoring system activity and diagnosing system breaches.

The audit log is stored by default in the /var/log/audit/ directory, within a file named audit.log. However, the location can be customized in the auditd.conf file. Each entry in the audit log is made up of several fields, including an event identifier, a timestamp, the user identity (UID), the event type, the success or failure of the event, and other information pertinent to the event such as the command run or the file accessed.

The command is a utility that generates reports from the audit daemon logs. It extracts information from the audit logs in a summarized format, making it easier for an administrator to review and analyze. For example, provides a list of audit event summaries related to executable files, while shows a list of all login-related events.

The command is another utility for searching the audit logs. Unlike , which generates summary reports, allows for searching specific details in the audit logs based on different search criteria like event time, user IDs, event types, and more. For example, would search for all login events generated by the user with UID 1000.

The audit.rules file, typically located at /etc/audit/audit.rules, is where the administrator defines what actions to capture. When the auditd service starts, it reads this file to determine what events to monitor. Good rules to capture often include file access and changes to critical system files, changes to user/group information, and usage of privileged commands. Rules can be made as broad or as specific as required, allowing a granular level of control over what information is logged.

Creating the audit.rules file requires a good understanding of the system and its security needs. It should be configured to capture enough information to be helpful for security audits without overwhelming the system or administrators with too much data. Rules should be tested to ensure they capture the required information and do not generate excessive false positives that could hide true security concerns.

In conclusion, auditd is a crucial tool in the arsenal of a Linux system administrator. It provides a robust framework for monitoring system activity that is critical for security and compliance. Properly configuring and maintaining the auditd service and its associated components ensures that valuable information is captured and stored securely, providing a key resource for understanding system events and detecting potential security incidents.

Want to know more?

This is a super quick summary, really just trying to show the key points. If you want to know more about this, there are a series of awesome blog posts by Rohit N. available at: https://izyknows.medium.com/linux-auditd-for-threat-detection-d06c8b941505

If you want some formal training on Linux IR, including analyzing AuditD files, then have a look at the SANS FOR577 Linux Incident Response Course - https://sans.org/for577.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858