**CHAPTER 7. SYSTEM AUDITING**

The Linux Audit system provides a way to track security-relevant information on your system. Based on pre-configured rules, Audit generates log entries to record as much information about the events that are happening on your system as possible. This information is crucial for mission-critical environments to determine the violator of the security policy and the actions they performed. Audit does not provide additional security to your system; rather, it can be used to discover violations of security policies used on your system. These violations can further be prevented by additional security measures such as SELinux.

The following list summarizes some of the information that Audit is capable of recording in its log files:

* Date and time, type, and outcome of an event.
* Sensitivity labels of subjects and objects.
* Association of an event with the identity of the user who triggered the event.
* All modifications to Audit configuration and attempts to access Audit log files.
* All uses of authentication mechanisms, such as SSH, Kerberos, and others.
* Changes to any trusted database, such as /etc/passwd.
* Attempts to import or export information into or from the system.
* Include or exclude events based on user identity, subject and object labels, and other attributes.

The use of the Audit system is also a requirement for a number of security-related certifications. Audit is designed to meet or exceed the requirements of the following certifications or compliance guides:

* Controlled Access Protection Profile (CAPP)
* Labeled Security Protection Profile (LSPP)
* Rule Set Base Access Control (RSBAC)
* National Industrial Security Program Operating Manual (NISPOM)
* Federal Information Security Management Act (FISMA)
* Payment Card Industry — Data Security Standard (PCI-DSS)
* Security Technical Implementation Guides (STIG)

Audit has also been:

* Evaluated by National Information Assurance Partnership (NIAP) and Best Security Industries (BSI).
* Certified to LSPP/CAPP/RSBAC/EAL4+ on Red Hat Enterprise Linux 5.
* Certified to Operating System Protection Profile / Evaluation Assurance Level 4+ (OSPP/EAL4+) on Red Hat Enterprise Linux 6.

Use Cases

**Watching file access**

Audit can track whether a file or a directory has been accessed, modified, executed, or the file's attributes have been changed. This is useful, for example, to detect access to important files and have an Audit trail available in case one of these files is corrupted.

**Monitoring system calls**

Audit can be configured to generate a log entry every time a particular system call is used. This can be used, for example, to track changes to the system time by monitoring the settimeofday, clock\_adjtime, and other time-related system calls.

**Recording commands run by a user**

Because Audit can track whether a file has been executed, a number of rules can be defined to record every execution of a particular command. For example, a rule can be defined for every executable in the /bin directory. The resulting log entries can then be searched by user ID to generate an audit trail of executed commands per user.

**Recording security events**

The pam\_faillock authentication module is capable of recording failed login attempts. Audit can be set up to record failed login attempts as well, and provides additional information about the user who attempted to log in.

**Searching for events**

Audit provides the **ausearch** utility, which can be used to filter the log entries and provide a complete audit trail based on a number of conditions.

**Running summary reports**

The **aureport** utility can be used to generate, among other things, daily reports of recorded events. A system administrator can then analyze these reports and investigate suspicious activity furthermore.

**Monitoring network access**

The **iptables** and **ebtables** utilities can be configured to trigger Audit events, allowing system administrators to monitor network access.

**Note:-**System performance may be affected depending on the amount of information that is collected by Audit.