Impair Defenses: Disable or Modify Linux Audit System, Sub-technique T1562.012 - Enterprise

Archived: 2026-04-05 12:53:10 UTC

Adversaries may disable or modify the Linux audit system to hide malicious activity and avoid detection. Linux admins use the Linux Audit system to track security-relevant information on a system. The Linux Audit system operates at the kernel-level and maintains event logs on application and system activity such as process, network, file, and login events based on pre-configured rules.

Often referred to as `auditd`, this is the name of the daemon used to write events to disk and is governed by the parameters set in the `audit.conf` configuration file. Two primary ways to configure the log generation rules are through the command line `auditctl` utility and the file `/etc/audit/audit.rules`, containing a sequence of `auditctl` commands loaded at boot time.[1][2]

With root privileges, adversaries may be able to ensure their activity is not logged through disabling the Audit system service, editing the configuration/rule files, or by hooking the Audit system library functions. Using the command line, adversaries can disable the Audit system service through killing processes associated with `auditd` daemon or use `systemctl` to stop the Audit service. Adversaries can also hook Audit system functions to disable logging or modify the rules contained in the `/etc/audit/audit.rules` or `audit.conf` files to ignore malicious activity.[3][4]

Source: https://attack.mitre.org/techniques/T1562/012