Sign in

Neo23x0 / **auditd** Public

Notifications Fork 258 Star 1.5k

Code Issues 15 Pull requests 25 Actions Projects Security Insights

auditd / **audit.rules**

Neo23x0 Merge branch 'master' into patch-63 ✓ 38e2780 · 2 weeks ago

818 lines (646 loc) · 31.1 KB

Code Blame Raw

```
#      ___             ___ __      __
#     /   | __  ______/ (_) /_____/ /
#    / /| |/ / / / __  / / __/ __  /
#   / ___ / /_/ / /_/ / / /_/ /_/ /
#  /_/  |_\__,_/\__,_/_/\__/\__,_/
#
# Linux Audit Daemon - Best Practice Configuration
# /etc/audit/audit.rules
#
# Compiled by Florian Roth
#
# Created  : 2017/12/05
# Modified : 2023/01/25
#
# Based on rules published here:
#   Gov.uk auditd rules
#       https://github.com/gds-operations/puppet-auditd/pull/1
#       CentOS 7 hardening
#               https://highon.coffee/blog/security-harden-centos-7/#auditd---audit-daemon
#       Linux audit repo
#               https://github.com/linux-audit/audit-userspace/tree/master/rules
#       Auditd high performance linux auditing
#               https://linux-audit.com/tuning-auditd-high-performance-linux-auditing/
#
# Further rules
#       For PCI DSS compliance see:
```

```
#               https://github.com/linux-audit/audit-userspace/blob/master/rules/30-pci-dss-v31.rul
#       For NISPOM compliance see:
#               https://github.com/linux-audit/audit-userspace/blob/master/rules/30-nispom.rules

# Remove any existing rules
-D

# Buffer Size
## Feel free to increase this if the machine panic's
-b 8192

# Failure Mode
## Possible values: 0 (silent), 1 (printk, print a failure message), 2 (panic, halt the system)
-f 1

# Ignore errors
## e.g. caused by users or files not found in the local environment
-i

# Self Auditing ---------------------------------------------------------------

## Audit the audit logs
### Successful and unsuccessful attempts to read information from the audit records
-w /var/log/audit/ -p wra -k auditlog
-w /var/audit/ -p wra -k auditlog

## Auditd configuration
### Modifications to audit configuration that occur while the audit collection functions are operat
-w /etc/audit/ -p wa -k auditconfig
-w /etc/libaudit.conf -p wa -k auditconfig
-w /etc/audisp/ -p wa -k audispconfig

## Monitor for use of audit management tools
-w /sbin/auditctl -p x -k audittools
-w /sbin/auditd -p x -k audittools
-w /usr/sbin/auditd -p x -k audittools
-w /usr/sbin/augenrules -p x -k audittools

## Access to all audit trails

-a always,exit -F path=/usr/sbin/ausearch -F perm=x -k audittools
-a always,exit -F path=/usr/sbin/aureport -F perm=x -k audittools
-a always,exit -F path=/usr/sbin/aulast -F perm=x -k audittools
-a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k audittools
-a always,exit -F path=/usr/sbin/auvirt -F perm=x -k audittools

```

```
# Filters ---------------------------------------------------------------------

### We put these early because audit is a first match wins system.

## Ignore current working directory records
-a always,exclude -F msgtype=CWD

## Cron jobs fill the logs with stuff we normally don't want (works with SELinux)
-a never,user -F subj_type=crond_t
-a never,exit -F subj_type=crond_t

## This prevents chrony from overwhelming the logs
-a never,exit -F arch=b64 -S adjtimex -F auid=-1 -F uid=chrony -F subj_type=chronyd_t

## This is not very interesting and wastes a lot of space if the server is public facing
-a always,exclude -F msgtype=CRYPTO_KEY_USER

## Open VM Tools
-a exit,never -F arch=b64 -S all -F exe=/usr/bin/vmtoolsd

## High Volume Event Filter (especially on Linux Workstations)
-a never,exit -F arch=b32 -F dir=/dev/shm/ -F key=sharedmemaccess
-a never,exit -F arch=b64 -F dir=/dev/shm/ -F key=sharedmemaccess

-a never,exit -F arch=b32 -F dir=/var/lock/lvm/ -F key=locklvm
-a never,exit -F arch=b64 -F dir=/var/lock/lvm/ -F key=locklvm

## Filebeat
### https://www.elastic.co/guide/en/beats/filebeat/current/directory-layout.html

-a never,exit -F arch=b32 -F path=/opt/filebeat -F perm=wa -F key=filebeat
-a never,exit -F arch=b64 -F path=/opt/filebeat -F perm=wa -F key=filebeat

-a always,exit -F arch=b32 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat
-a always,exit -F arch=b64 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat

-a always,exit -F arch=b32 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat
-a always,exit -F arch=b64 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat

-a always,exit -F arch=b64 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat
-a always,exit -F arch=b32 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat

### macOS
#### https://www.elastic.co/guide/en/beats/filebeat/7.17/directory-layout.html
-a always,exit -F arch=b32 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm=x -F key=fi
-a always,exit -F arch=b64 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm=x -F key=fi
```

```
-a always,exit -F arch=b64 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm=x -F key=fi
```

```
# ipc system call
# /usr/include/linux/ipc.h

## msgctl
#-a always,exit -S ipc -F a0=14 -k Inter-Process_Communication
## msgget
#-a always,exit -S ipc -F a0=13 -k Inter-Process_Communication
## Use these lines on x86_64, ia64 instead
-a always,exit -F arch=b64 -S msgctl -k Inter-Process_Communication
-a always,exit -F arch=b64 -S msgget -k Inter-Process_Communication

## semctl
#-a always,exit -S ipc -F a0=3 -k Inter-Process_Communication
## semget
#-a always,exit -S ipc -F a0=2 -k Inter-Process_Communication
```

```
## semop
#-a always,exit -S ipc -F a0=1 -k Inter-Process_Communication
## semtimedop
#-a always,exit -S ipc -F a0=4 -k Inter-Process_Communication
## Use these lines on x86_64, ia64 instead
-a always,exit -F arch=b64 -S semctl -k Inter-Process_Communication
-a always,exit -F arch=b64 -S semget -k Inter-Process_Communication
-a always,exit -F arch=b64 -S semop -k Inter-Process_Communication
-a always,exit -F arch=b64 -S semtimedop -k Inter-Process_Communication

## shmctl
#-a always,exit -S ipc -F a0=24 -k Inter-Process_Communication
## shmget
#-a always,exit -S ipc -F a0=23 -k Inter-Process_Communication
## Use these lines on x86_64, ia64 instead
-a always,exit -F arch=b64 -S shmctl -k Inter-Process_Communication
-a always,exit -F arch=b64 -S shmget -k Inter-Process_Communication

# High Volume Events ----------------------------------------------------------

## Disable these rules if they create too many events in your environment

## Common Shells
-w /bin/bash -p x -k susp_shell
-w /bin/dash -p x -k susp_shell
-w /bin/busybox -p x -k susp_shell
-w /bin/zsh -p x -k susp_shell
-w /bin/sh -p x -k susp_shell
-w /bin/ksh -p x -k susp_shell

## Root command executions
-a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=-1 -S execve -k rootcmd

## File Deletion Events by User
-a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F au

## File Access
### Unauthorized Access (unsuccessful)
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate

### Unsuccessful Creation
-a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -F exit=-EACC
-a always,exit -F arch=b64 -S mkdir,link,symlink,mkdirat -F exit=-EPERM -k file_creation

### Unsuccessful Modification
```

```
### Unsuccessful Modification
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S r
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S r

## 32bit API Exploitation
### If you are on a 64 bit platform, everything _should_ be running
### in 64 bit mode. This rule will detect any use of the 32 bit syscalls
### because this might be a sign of someone exploiting a hole in the 32
### bit API.
-a always,exit -F arch=b32 -S all -k 32bit_api

# Make The Configuration Immutable --------------------------------------------

##-e 2
```