

Files

🔑 master 🔍

🔍 Go to file

> .github

LICENSE

README.md

audit.rules

auditd / audit.rules

 Neo23x0 Merge branch 'master' into patch-63 ✓

38e2780 · 2 weeks ago🕒 History

CodeBlame818 lines (646 loc) · 31.1 KB

Raw📄📥🔧⌵🔍

```
1  #
2  #   ____  ____  ____
3  #   /  |  _  ____/ ( ) /____/ /
4  #   /  | /  / /  _  /  _  /
5  #   /  | /  / /  _  /  _  /
6  #   /  | /  / /  _  /  _  /
7  #   /  | /  / /  _  /  _  /
8  #   /  | /  / /  _  /  _  /
9  #   /  | /  / /  _  /  _  /
10 #   /  | /  / /  _  /  _  /
11 #   /  | /  / /  _  /  _  /
12 #   /  | /  / /  _  /  _  /
13 #   /  | /  / /  _  /  _  /
14 #   /  | /  / /  _  /  _  /
15 #   /  | /  / /  _  /  _  /
16 #   /  | /  / /  _  /  _  /
17 #   /  | /  / /  _  /  _  /
18 #   /  | /  / /  _  /  _  /
19 #   /  | /  / /  _  /  _  /
20 #   /  | /  / /  _  /  _  /
21 #   /  | /  / /  _  /  _  /
22 #   /  | /  / /  _  /  _  /
23 #   /  | /  / /  _  /  _  /
24 #   /  | /  / /  _  /  _  /
25 #   /  | /  / /  _  /  _  /
26 #   /  | /  / /  _  /  _  /
27 #   /  | /  / /  _  /  _  /
28 #   /  | /  / /  _  /  _  /
29 #   /  | /  / /  _  /  _  /
30 #   /  | /  / /  _  /  _  /
31 #   /  | /  / /  _  /  _  /
32 #   /  | /  / /  _  /  _  /
33 #   /  | /  / /  _  /  _  /
34 #   /  | /  / /  _  /  _  /
35 #   /  | /  / /  _  /  _  /
36 #   /  | /  / /  _  /  _  /
37 #   /  | /  / /  _  /  _  /
38 #   /  | /  / /  _  /  _  /
39 #   /  | /  / /  _  /  _  /
40 #   /  | /  / /  _  /  _  /
41 #   /  | /  / /  _  /  _  /
42 #   /  | /  / /  _  /  _  /
43 #   /  | /  / /  _  /  _  /
44 #   /  | /  / /  _  /  _  /
45 #   /  | /  / /  _  /  _  /
46 #   /  | /  / /  _  /  _  /
47 #   /  | /  / /  _  /  _  /
48 #   /  | /  / /  _  /  _  /
49 #   /  | /  / /  _  /  _  /
50 #   /  | /  / /  _  /  _  /
51 #   /  | /  / /  _  /  _  /
52 #   /  | /  / /  _  /  _  /
53 #   /  | /  / /  _  /  _  /
54 #   /  | /  / /  _  /  _  /
55 #   /  | /  / /  _  /  _  /
56 #   /  | /  / /  _  /  _  /
57 #   /  | /  / /  _  /  _  /
```

```
57     -w /etc/auditp/ -p wa -k auditpconfig
58
59     ## Monitor for use of audit management tools
60     -w /sbin/auditctl -p x -k audittools
61     -w /sbin/auditd -p x -k audittools
62     -w /usr/sbin/auditd -p x -k audittools
63     -w /usr/sbin/augenrules -p x -k audittools
64
65     ## Access to all audit trails
66
67     -a always,exit -F path=/usr/sbin/ausearch -F perm=x -k audittools
68     -a always,exit -F path=/usr/sbin/aureport -F perm=x -k audittools
69     -a always,exit -F path=/usr/sbin/aulast -F perm=x -k audittools
70     -a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k audittools
71     -a always,exit -F path=/usr/sbin/auvirt -F perm=x -k audittools
72
73     # Filters -----
74
75     ### We put these early because audit is a first match wins system.
76
77     ## Ignore current working directory records
78     -a always,exclude -F msgtype=CWD
79
80     ## Cron jobs fill the logs with stuff we normally don't want (works with SELinux)
81     -a never,user -F subj_type=crond_t
82     -a never,exit -F subj_type=crond_t
83
84     ## This prevents chrony from overwhelming the logs
85     -a never,exit -F arch=b64 -S adjtimex -F auid=-1 -F uid=chrony -F subj_type=chronyd_t
86
87     ## This is not very interesting and wastes a lot of space if the server is public facing
88     -a always,exclude -F msgtype=CRYPTO_KEY_USER
89
90     ## Open VM Tools
91     -a exit,never -F arch=b64 -S all -F exe=/usr/bin/vmtoolsd
92
93     ## High Volume Event Filter (especially on Linux Workstations)
94     -a never,exit -F arch=b32 -F dir=/dev/shm/ -F key=sharedmemaccess
95     -a never,exit -F arch=b64 -F dir=/dev/shm/ -F key=sharedmemaccess
96
97     -a never,exit -F arch=b32 -F dir=/var/lock/lvm/ -F key=locklvm
98     -a never,exit -F arch=b64 -F dir=/var/lock/lvm/ -F key=locklvm
99
100    ## Filebeat
101    ### https://www.elastic.co/guide/en/beats/filebeat/current/directory-layout.html
102
103    -a never,exit -F arch=b32 -F path=/opt/filebeat -F perm=wa -F key=filebeat
104    -a never,exit -F arch=b64 -F path=/opt/filebeat -F perm=wa -F key=filebeat
105
106    -a always,exit -F arch=b32 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat
107    -a always,exit -F arch=b64 -F dir=/etc/filebeat/ -F perm=wa -F key=filebeat
108
109    -a always,exit -F arch=b32 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat
110    -a always,exit -F arch=b64 -F dir=/usr/share/filebeat/ -F perm=wa -F key=filebeat
111
112    -a always,exit -F arch=b64 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat
113    -a always,exit -F arch=b32 -F dir=/usr/share/filebeat/bin/ -F perm=x -F key=filebeat
114
115    ### macOS
116    #### https://www.elastic.co/guide/en/beats/filebeat/7.17/directory-layout.html
117    -a always,exit -F arch=b32 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm=wa -F key=filebeat
118    -a always,exit -F arch=b64 -F path=/usr/local/var/homebrew/linked/filebeat-full -F perm=wa -F key=filebeat
```



```
745     # ipc system call
746     # /usr/include/linux/ipc.h
747
748     ## msgctl
749     #-a always,exit -S ipc -F a0=14 -k Inter-Process_Communication
750     ## msgget
751     #-a always,exit -S ipc -F a0=13 -k Inter-Process_Communication
752     ## Use these lines on x86_64, ia64 instead
753     -a always,exit -F arch=b64 -S msgctl -k Inter-Process_Communication
754     -a always,exit -F arch=b64 -S msgget -k Inter-Process_Communication
755
756     ## semctl
757     #-a always,exit -S ipc -F a0=3 -k Inter-Process_Communication
758     ## semget
759     #-a always,exit -S ipc -F a0=2 -k Inter-Process_Communication
760     ## semop
761     #-a always,exit -S ipc -F a0=1 -k Inter-Process_Communication
762     ## semtimedop
763     #-a always,exit -S ipc -F a0=4 -k Inter-Process_Communication
764     ## Use these lines on x86_64, ia64 instead
765     -a always,exit -F arch=b64 -S semctl -k Inter-Process_Communication
766     -a always,exit -F arch=b64 -S semget -k Inter-Process_Communication
767     -a always,exit -F arch=b64 -S semop -k Inter-Process_Communication
768     -a always,exit -F arch=b64 -S semtimedop -k Inter-Process_Communication
769
770     ## shmctl
771     #-a always,exit -S ipc -F a0=24 -k Inter-Process_Communication
772     ## shmget
773     #-a always,exit -S ipc -F a0=23 -k Inter-Process_Communication
774     ## Use these lines on x86_64, ia64 instead
775     -a always,exit -F arch=b64 -S shmctl -k Inter-Process_Communication
776     -a always,exit -F arch=b64 -S shmget -k Inter-Process_Communication
777
778     # High Volume Events -----
779
780     ## Disable these rules if they create too many events in your environment
781
782     ## Common Shells
783     -w /bin/bash -p x -k susp_shell
784     -w /bin/dash -p x -k susp_shell
785     -w /bin/busybox -p x -k susp_shell
786     -w /bin/zsh -p x -k susp_shell
787     -w /bin/sh -p x -k susp_shell
788     -w /bin/ksh -p x -k susp_shell
789
790     ## Root command executions
791     -a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=-1 -S execve -k rootcmd
792
793     ## File Deletion Events by User
794     -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid
795
796     ## File Access
797     ### Unauthorized Access (unsuccessful)
798     -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate
799     -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate
800
801     ### Unsuccessful Creation
802     -a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -
803     -a always,exit -F arch=b64 -S mkdir,link,symlink,mknod,mknodat -F auid=0 -F euid=0 -k file_creatio
```

```
803     -a always,exit -F arch=b64 -S unlink,link,symlink,mknod -F exit=-EPERM -k file_creation
804
805     ### Unsuccessful Modification
806     -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S ls
807     -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S ls
808
809     ## 32bit API Exploitation
810     ### If you are on a 64 bit platform, everything _should_ be running
811     ### in 64 bit mode. This rule will detect any use of the 32 bit syscalls
812     ### because this might be a sign of someone exploiting a hole in the 32
813     ### bit API.
814     -a always,exit -F arch=b32 -S all -k 32bit_api
815
816     # Make The Configuration Immutable -----
817
818     ##-e 2
```