How to Secure RHEL 7.1
Part 4

Motivation

This paper is part of a multi-part series on securing CentOS 7.1. This paper focuses on the setup, configuration and routine appraisal of the auditing logs. When you setup the server, you need to create a separate partition for the audit logs, the default for this is /var/log/audit, I prefer to use /security1 for my OS audit logs and /security2 for my application audit logs. If size permits, I prefer to have 16GB for each of these. If size is a problem, set them minimally to 4GB each.

Audit Daemon (auditd)

Installation

Use either YUM or RPM to install the auditd software package. Mount the DVD RHEL 7.1 distribution and change directory to the Package directory.

```
# mount /media/cdrom
# cd /media/cdrom/Packages
# yum install auditd*
```

Configuration

Copy the following content into /etc/audit/auditd.conf:

```
##
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
#
priority_boost = 4
flush = INCREMENTAL
freq = 20
#
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
#
max_log_file = 100
max_log_file_action = ROTATE
#
space_left = 125
space_left_action = SUSPEND
#
action_mail_acct = root
```

```
#
admin_space_left = 75
admin_space_left_action = SUSPEND
#
disk_full_action = HALT
disk_error_action = SUSPEND
#
tcp_listen_queue = 5
tcp_max_per_addr = 1
tcp_client_max_idle = 0
#
enable_krb5 = no
krb5_principal = auditd
```

Copy the following content into /etc/audit/audit.rules:

```
## This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.
#
#
# First rule - delete all
-D
# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 16384
##
#     the panic failure flag -f 2 ensures that your
#     audit records are complete even if the system
#     is encountering critical errors:
-f 2
##
#     Failed file & program access attempts:
-a exit,always -F arch=b64 -S open -F success!=0
##
#     Audit file & program deletion:
-a always,exit -F arch=b64 -S mkdir
-a always,exit -F arch=b64 -S rmdir
-a always,exit -F arch=b64 -S unlink
##
#     Audit administrative, privleaged, and security options:
-w /bin/su
-w /usr/bin/passwd
-w /usr/bin/sudo
##
#     Audit DACL modifications:
-a always,exit -F arch=b64 -S chmod
-a always,exit -F arch=b64 -S fchmod
-a always,exit -F arch=b64 -S chown
-a always,exit -F arch=b64 -S fchown
-a always,exit -F arch=b64 -S lchown
-a always,exit -F arch=b64 -S truncate
-a always,exit -F arch=b64 -S ftruncate
-a always,exit -F arch=b64 -S rename
-a always,exit -F arch=b64 -S link
```

```
-a always,exit -F arch=b64 -S symlink
-a always,exit -F arch=b64 -S setxattr
-a always,exit -F arch=b64 -S lsetxattr
-a always,exit -F arch=b64 -S fsetxattr
-a always,exit -F arch=b64 -S removexattr
-a always,exit -F arch=b64 -S lremovexattr
-a always,exit -F arch=b64 -S fremovexattr
-a always,exit -F arch=b64 -S mknod
-a always,exit -F arch=b64 -S mount
-a always,exit -F arch=b64 -S umount2
##
#     Login-logout & session initialization:
-w /bin/login
##
#     Monitoring Miscellaneous System Calls:
-a always,exit -F arch=b64 -S clone
-a always,exit -F arch=b64 -S fork
-a always,exit -F arch=b64 -S vfork
-a always,exit -F arch=b64 -S umask
-a always,exit -F arch=b64 -S adjtimex
-a always,exit -F arch=b64 -S settimeofday
##
#    Add your files to monitor below this line:
-w /var/log/audit/
-w /var/log/audit/audit.log
-w /etc/audit/auditd.conf -p wa
-w /var/run/utmp -p wa -k session
-w /var/log/btmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /etc/audit/audit.rules -p wa
-w /etc/libaudit.conf -p wa
-w /etc/sysconfig/auditd -p wa
-w /var/spool/atspool
-w /etc/at.allow
-w /etc/at.deny
#
-w /etc/cron.allow -p wa
-w /etc/cron.deny -p wa
-w /etc/cron.d/ -p wa
-w /etc/cron.daily/ -p wa
-w /etc/cron.hourly/ -p wa
-w /etc/cron.monthly/ -p wa
-w /etc/cron.weekly/ -p wa
-w /etc/crontab -p wa
-w /var/spool/cron/root
#
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
#
-w /etc/login.defs -p wa
-w /etc/securetty
-w /var/log/faillog
-w /var/log/lastlog
#
```

```
-w /etc/hosts -p wa
-w /etc/sysconfig/
#
-w /etc/inittab -p wa
-w /etc/init.d/
-w /etc/init.d/auditd -p wa
#
-w /etc/ld.so.conf -p wa
#
-w /etc/localtime -p wa
#
-w /etc/sysctl.conf -p wa
#
-w /etc/modprobe.d/
-w /etc/modprobe.conf.local -p wa
-w /etc/modprobe.conf -p wa
#
-w /etc/pam.d/
#
-w /etc/aliases -p wa
-w /etc/postfix/ -p wa
#
-w /etc/ssh/sshd_config
#
-w /etc/stunnel/stunnel.conf
-w /etc/stunnel/stunnel.pem
#
-w /etc/vsftpd.ftpusers
-w /etc/vsftpd.conf
#
-a exit,always -F arch=b64 -S sethostname
-a exit,always -F arch=b64 -S setdomainname
-w /etc/issue -p wa
-w /etc/issue.net -p wa
```

Search Audit Logs

ausearch

A command that can query the audit daemon logs based for events based on different search criteria.

If I wanted to see who touched or modified /etc/passwd, I would use:

```
ausearch -f /etc/passwd -i
```

Output:

```
type=PATH msg=audit(11/22/2015 16:37:01.143:65089) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:01.143:65089) :  cwd=/
type=SYSCALL msg=audit(11/22/2015 16:37:01.143:65089) : arch=x86_64
syscall=open success=yes exit=6 a0=7f9f9ead669a a1=80000 a2=1b6 a3=0 items=1
ppid=1 pid=1888 auid=unset uid=root gid=root euid=root suid=root fsuid=root
egid=root sgid=root fsgid=root tty=(none) ses=unset comm=crond
exe=/usr/sbin/crond key=(null)
----
```

```
type=PATH msg=audit(11/22/2015 16:37:01.143:65090) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:01.143:65090) :  cwd=/
type=SYSCALL msg=audit(11/22/2015 16:37:01.143:65090) : arch=x86_64
syscall=open success=yes exit=6 a0=7f9f9ead669a a1=80000 a2=1b6 a3=0 items=1
ppid=1 pid=1888 auid=unset uid=root gid=root euid=root suid=root fsuid=root
egid=root sgid=root fsgid=root tty=(none) ses=unset comm=crond
exe=/usr/sbin/crond key=(null)
----
type=PATH msg=audit(11/22/2015 16:37:01.143:65091) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:01.143:65091) :  cwd=/
type=SYSCALL msg=audit(11/22/2015 16:37:01.143:65091) : arch=x86_64
syscall=open success=yes exit=6 a0=7f9f9ead669a a1=80000 a2=1b6 a3=0 items=1
ppid=1 pid=1888 auid=unset uid=root gid=root euid=root suid=root fsuid=root
egid=root sgid=root fsgid=root tty=(none) ses=unset comm=crond
exe=/usr/sbin/crond key=(null)
----
type=PATH msg=audit(11/22/2015 16:37:01.143:65092) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:01.143:65092) :  cwd=/
type=SYSCALL msg=audit(11/22/2015 16:37:01.143:65092) : arch=x86_64
syscall=open success=yes exit=6 a0=7f9f9ead669a a1=80000 a2=1b6 a3=0 items=1
ppid=1 pid=1888 auid=unset uid=root gid=root euid=root suid=root fsuid=root
egid=root sgid=root fsgid=root tty=(none) ses=unset comm=crond
exe=/usr/sbin/crond key=(null)
----
type=PATH msg=audit(11/22/2015 16:37:37.382:65152) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:37.382:65152) :  cwd=/etc/audit
type=SYSCALL msg=audit(11/22/2015 16:37:37.382:65152) : arch=x86_64
syscall=open success=yes exit=4 a0=7ffc2328769a a1=80000 a2=1b6 a3=0 items=1
ppid=2032 pid=4721 auid=masterf uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=3 comm=ausearch
exe=/sbin/ausearch key=(null)
----
type=PATH msg=audit(11/22/2015 16:37:37.383:65154) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:37.383:65154) :  cwd=/etc/audit
type=SYSCALL msg=audit(11/22/2015 16:37:37.383:65154) : arch=x86_64
syscall=open success=yes exit=4 a0=7ffc2328769a a1=80000 a2=1b6 a3=0 items=1
ppid=2032 pid=4721 auid=masterf uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=3 comm=ausearch
exe=/sbin/ausearch key=(null)
----
type=PATH msg=audit(11/22/2015 16:37:37.556:65156) : item=0 name=/etc/passwd
inode=3001 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(11/22/2015 16:37:37.556:65156) :  cwd=/etc/audit
type=SYSCALL msg=audit(11/22/2015 16:37:37.556:65156) : arch=x86_64
syscall=open success=yes exit=4 a0=7ffc2328769a a1=80000 a2=1b6 a3=0 items=1
ppid=2032 pid=4721 auid=masterf uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=3 comm=ausearch
exe=/sbin/ausearch key=(null)
```

Search for recent events:

```
ausearch -ts recent
```

Output:

```
----
time->Thu Nov 22 17:04:09 2015
type=PATH msg=audit(1353621849.809:69732): item=0 name="/proc/net/ipv6_route"
inode=4026532501 dev=00:03 mode=0100444 ouid=0 ogid=0 rdev=00:00
type=CWD msg=audit(1353621849.809:69732):  cwd="/"
type=SYSCALL msg=audit(1353621849.809:69732): arch=c000003e syscall=2
success=yes exit=19 a0=7f4c1556f760 a1=0 a2=1 a3=15 items=1 ppid=1 pid=1552
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="vmtoolsd" exe="/usr/lib/vmware-
tools/sbin64/vmtoolsd" key=(null)
----
time->Thu Nov 22 17:04:09 2015
type=PATH msg=audit(1353621849.809:69733): item=0 name="/proc/uptime"
inode=4026532033 dev=00:03 mode=0100444 ouid=0 ogid=0 rdev=00:00
type=CWD msg=audit(1353621849.809:69733):  cwd="/"
type=SYSCALL msg=audit(1353621849.809:69733): arch=c000003e syscall=2
success=yes exit=19 a0=196d9e0 a1=0 a2=1b6 a3=0 items=1 ppid=1 pid=1552
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="vmtoolsd" exe="/usr/lib/vmware-
tools/sbin64/vmtoolsd" key=(null)
----
time->Thu Nov 22 17:04:09 2015
type=PATH msg=audit(1353621849.810:69734): item=0 name="/proc/meminfo"
inode=4026532031 dev=00:03 mode=0100444 ouid=0 ogid=0 rdev=00:00
type=CWD msg=audit(1353621849.810:69734):  cwd="/"
type=SYSCALL msg=audit(1353621849.810:69734): arch=c000003e syscall=2
success=yes exit=19 a0=7f4c15570152 a1=0 a2=1b6 a3=0 items=1 ppid=1 pid=1552
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="vmtoolsd" exe="/usr/lib/vmware-
tools/sbin64/vmtoolsd" key=(null)
----
```

Now, lets say that I want to know who or what process messed with /var/log/audit/audit.log within the last month, I would run:

```
ausearch -ts this-month -f /var/log/audit/audit.log
```

Output:

```
----
time->Thu Nov 22 17:08:38 2015
type=PATH msg=audit(1353622118.000:70314): item=0
name="/var/log/audit/audit.log" inode=261712 dev=08:09 mode=0100600 ouid=0
ogid=0 rdev=00:00
type=CWD msg=audit(1353622118.000:70314):  cwd="/etc/audit"
type=SYSCALL msg=audit(1353622118.000:70314): arch=c000003e syscall=2
success=yes exit=4 a0=7fff92c367db a1=0 a2=336c39ced8 a3=8028 items=1
ppid=2032 pid=4826 auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
fsgid=0 tty=pts0 ses=3 comm="ausearch" exe="/sbin/ausearch" key=(null)
----
time->Thu Nov 22 17:08:38 2015
type=PATH msg=audit(1353622118.004:70319): item=0
name="/var/log/audit/audit.log.2" inode=261672 dev=08:09 mode=0100400 ouid=0
ogid=0 rdev=00:00
type=CWD msg=audit(1353622118.004:70319):  cwd="/etc/audit"
```

```
type=SYSCALL msg=audit(1353622118.004:70319): arch=c000003e syscall=2
success=yes exit=3 a0=1b0c800 a1=0 a2=1b6 a3=1 items=1 ppid=2032 pid=4826
auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0
ses=3 comm="ausearch" exe="/sbin/ausearch" key=(null)
----
time->Thu Nov 22 17:08:38 2015
type=PATH msg=audit(1353622118.316:70320): item=0
name="/var/log/audit/audit.log.1" inode=261711 dev=08:09 mode=0100400 ouid=0
ogid=0 rdev=00:00
type=CWD msg=audit(1353622118.316:70320):  cwd="/etc/audit"
type=SYSCALL msg=audit(1353622118.316:70320): arch=c000003e syscall=2
success=yes exit=3 a0=1b0c800 a1=0 a2=1b6 a3=1 items=1 ppid=2032 pid=4826
auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0
ses=3 comm="ausearch" exe="/sbin/ausearch" key=(null)
----
time->Thu Nov 22 17:08:38 2015
type=PATH msg=audit(1353622118.710:70321): item=0
name="/var/log/audit/audit.log" inode=261712 dev=08:09 mode=0100600 ouid=0
ogid=0 rdev=00:00
type=CWD msg=audit(1353622118.710:70321):  cwd="/etc/audit"
type=SYSCALL msg=audit(1353622118.710:70321): arch=c000003e syscall=2
success=yes exit=3 a0=1b0c800 a1=0 a2=1b6 a3=1 items=1 ppid=2032 pid=4826
auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0
ses=3 comm="ausearch" exe="/sbin/ausearch" key=(null)
----
```

To understand what capabilities ausearch has that would pertain to a systems administrator, run:

```
man 8 ausearch
```

Conclusion

The simple answer for why you are implementing this is that it allows you to know what is occurring on your server. As an administrator, you need to set some time aside each week to review the audit logs on every server. The reason for this is that you will learn what occurs on each server (which is a baseline) and quickly recognize when an event occurs out of the norm. The audit logs will then allow you to recreate the event. From this information, you should be able to determine the attack vector, what the intruder did from the point of entering the system (what was compromised), how to clean up the attack and how to create a remediation plan to prevent future attacks of the same nature.