Аудит Linux

Опубликовано : 03.12.2017 **By** cryptoparty

Areas	Core	Resources	Services	Environment
System Hardening	Boot Process Containers Frameworks **Kernel** Service Manager Virtualization	Accounting **Authentication** Cryptography Logging Network Software Storage Time	Database Mail Middleware Monitoring Printing **Shell** **Web**	Forensics Incident Response Malware Risks Security Monitoring System Integrity
Security Auditing				
Compliance				

Аудит ИБ Закрытие уязвимостей Мануал

Один из основных столпов практической безопасности — аудит событий.

Без него просто немыслим разбор инцидентов и проведение криминалистических исследований. Не говоря уже о просто нарушении политик безопасности.

В Linux, помимо встроенного syslog и его усовершенствованных последователей, есть демон auditd, специально заточенный на регистрацию событий, связанных с различными видами доступа. Установить auditd можно начиная с ядра 2.6 в любом дистрибутиве.

Auditd позволяет вести слежение за такими событиями, как:
— Запуск и завершение работы системы (перезагрузка, остановка);
— Чтение/запись или изменение прав доступа к файлам;
— Инициация сетевого соединения или изменение сетевых настроек;
— Изменение информации о пользователе или группе;
— Изменение даты и времени;
— Запуск и остановка приложений;
— Выполнение системных вызовов.

Одна из фич auditd — запуск уже вместе с ядром.

Для того, чтобы его активировать, нужно добавить опцию audit=1 в параметры загрузчика.

При установке auditd не регистрирует ничего.

Для его работы требуется настроить правила в файле /etc/audit/audit.rules.

К счастью эксперты по безопасности составили рекомендуемый набор правил, который позволит отслеживать доступ ко всем значимым дефолтным функциям системы.

Списки правил

Для 64-битных систем

Рекомендованный экспертами базовый набор правил для 64-битных систем такой:

-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change

-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

-a always,exit -F arch=b64 -S clock_settime -k time-change

-a always,exit -F arch=b32 -S clock_settime -k time-change -w /etc/localtime -p wa -k time-change

-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

-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale

-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale

-w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale

-w /etc/hosts -p wa -k system-locale

-w /etc/network -p wa -k system-locale

-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins

-w /var/run/utmp -p wa -k session

-w /var/log/wtmp -p wa -k session

-w /var/log/btmp -p wa -k session

-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k mounts -a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k mounts

-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete

-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete

-w /etc/sudoers -p wa -k scope

-w /var/log/sudo.log -p wa -k actions

-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

-w /etc/audit/auditd.conf -p wa -k change-audit-cfg

-w /etc/audit/audit.rules -p wa -k change-audit-cfg

После чего выполнить команду:

*find **<file_system>** -xdev \(-perm -4000 -o -perm -2000 \) -type f | awk ‘{print «-a always,exit -F path=» $1 » -F perm=x -F auid>=500 -F auid!=4294967295 -k privileged» }’*

и результат тоже добавить в audit.rules.

Последней строкой должна быть директива:

-e 2

которая не позволит изменит правила аудита без перезагрузки.

Для 32-битных систем

Рекомендованный экспертами базовый набор правил для 32-битных систем такой:

-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change

-a always,exit -F arch=b32 -S clock_settime -k time-change -w /etc/localtime -p wa -k time-change

-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

-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale

-w /etc/issue -p wa -k system-locale

-w /etc/issue.net -p wa -k system-locale

-w /etc/hosts -p wa -k system-locale

-w /etc/network -p wa -k system-locale

-w /var/log/faillog -p wa -k logins

-w /var/log/lastlog -p wa -k logins

-w /var/log/tallylog -p wa -k logins

-w /var/run/utmp -p wa -k session

-w /var/log/wtmp -p wa -k session

-w /var/log/btmp -p wa -k session

-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k mounts

-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 -F auid!=4294967295 -k delete

-w /etc/sudoers -p wa -k scope

-w /var/log/sudo.log -p wa -k actions

-w /sbin/insmod -p x -k modules

-w /sbin/rmmod -p x -k modules

-w /sbin/modprobe -p x -k modules

-a always,exit -F arch=b32 -S init_module -S delete_module -k modules

-w /etc/audit/auditd.conf -p wa -k change-audit-cfg

-w /etc/audit/audit.rules -p wa -k change-audit-cfg

После чего выполнить команду:

find ***<file_system>*** *-xdev \(-perm -4000 -o -perm -2000 \) -type f | awk ‘{print «-a always,exit -F path=» $1 » -F perm=x -F auid>=500 -F auid!=4294967295 -k privileged» }’*

и результат тоже добавить в audit.rules.

Последней строкой должна быть директива:

-e 2

которая не позволит изменит правила аудита без перезагрузки.