

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

**«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

**ОТЧЕТ**

**О ПРАКТИЧЕСКОЙ РАБОТЕ №2**

по дисциплине «Безопасность операционных систем»

**«Настройка аудита ОС»**

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 14 декабря 2023 г.

Преподаватель:

Смирнов Данил Вадимович

«\_\_» \_\_\_\_\_ 2023 г.

Москва, 2023

## Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Ход работы</b>	<b>3</b>
2.1	Рекомендуемые правила . . . . .	3
2.2	События входа и выхода . . . . .	5
2.3	Управление учётными записями . . . . .	5
2.4	Аудит изменения политики . . . . .	6
2.5	Аудит использования привилегий . . . . .	8
2.6	Аудит доступа пользователя к объектам . . . . .	8
<b>3</b>	<b>Выводы о проделанной работе</b>	<b>9</b>

## 1 Цель работы

Целью работы является изучение основных политик, их подкатегорий и процесса настройки расширенной политики аудита.

## 2 Ход работы

### 2.1 Рекомендуемые правила

Для системы auditd существуют рекомендуемые правила (<https://github.com/Neo23x0/auditd/blob/master/audit.rules>). Эти правила содержат настройки для аудита следующих действий:

- Доступ к логам auditd (успех и неуспех)
- Доступ к правилам auditd (файлы конфигурации и утилиты)
- Доступ к параметрам ядра sysctl
- Доступ к модулям ядра: insmod, modprobe, rmmod, файлы конфигурации
- Монтирование mount
- Файл подкачки: swapon, swapoff
- Служба времени: adjtimex, settimeofday, clock\_settime, /etc/localtime
- Stunnel
- Cron: /etc/crontab
- Пользователи, группы, пароли: /etc/group, /etc/passwd, /etc/shadow
- Sudo: /etc/sudoers
- Psswd: /usr/bin/passwd
- Изменение групп: groupadd, groupmod, addgroup, useradd, userdel, usermod, adduser
- Сеть: sethostname, setdomainname
- Удалённая консоль: /bin/bash connect
- Успешные ipv4 и ipv6 подключения
- Файлы: /etc/hosts, /etc/sysconfig/network, /etc/network
- Init
- Пути к подключаемым библиотекам: /etc/ld.so.conf, /etc/ld.so.preload
- Настройки Pам, Mail
- SSH: /etc/ssh/sshd\_config, /root/.ssh
- Systemd: /bin/systemctl, /etc/systemd/
- SELinux
- Ошибки доступа к каталогам в корне файловой системы
- Повышение привилегий: su, sudo

- Питание: shutdown, poweroff, reboot, halt
- Сессии: utmp, btmp, wtmp
- Дискреционный доступ: chmod, chown etc.
- Правила на разведку, на подозрительную активность, работу с архивами
- Нестандартные командные оболочки, профили оболочек
- Инъекция кода с ptrace
- Анонимное создание файлов
- Доступ администраторов в чужие рабочие директории
- Создание сокетов
- Использование пакетных менеджеров
- Grep
- Docker и виртуализация (qemu, virtual box)
- kubelet
- Запуск команд под рутом
- Неуспех доступа к файлам

Установим правила (рисунки 1-3):

```
root@alex-nb /e/a/rules.d# wget https://raw.githubusercontent.com/Neo23x0/auditd/master/audit.rules -O recommended.rules
--2023-12-16 21:43:34-- https://raw.githubusercontent.com/Neo23x0/auditd/master/audit.rules
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27367 (27K) [text/plain]
Saving to: 'recommended.rules'

recommended.rules      100%[=====] 26.73K  --.-KB/s   in 0.03s

2023-12-16 21:43:35 (805 KB/s) - 'recommended.rules' saved [27367/27367]

root@alex-nb /e/a/rules.d# augenrules --load
No rules
enabled 1
failure 1
pid 32110
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 18000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 32110
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 18000
backlog_wait_time_actual 0
Unknown user: chrony
```

Рисунок 1 – Сохранение правил в файл

```
root@alex-nb /e/a/rules.d# auditctl -R /etc/audit/audit.rules
No rules
enabled 1
failure 1
pid 32110
```

Рисунок 2 – Применение правил

```
root@alex-nb /e/a/rules.d# auditctl -l | wc -l
358
root@alex-nb /e/a/rules.d#
```

Рисунок 3 – Количество активных правил

Рассмотрим основные действия, которые можно логировать, и изучим, как рекомендуемые правила справляются в рассматриваемых случаях.

## 2.2 События входа и выхода

Для логирования событий входа и выхода подойдёт следующий участок правил:

```
## Session initiation information
-w /var/run/utmp -p wa -k session
-w /var/log/btmp -p wa -k session
-w /var/log/wtmp -p wa -k session
```

Листинг 1 – События входа и выхода

Файл utmp содержит данные о текущей сессии, btmp — об ошибках, wtmp — история сессий. Сделаем поиск событий по ключу session. Видно, что последний вход под пользователем test осуществлялся в 22:20 (рисунок 4). В это время есть логи аудита (рисунок 5):

```
root@alex-nb -# who
alex    seat0      2023-12-16 21:56 (login screen)
alex    tty2        2023-12-16 21:56 (tty2)
alex    pts/2       2023-12-16 21:58
alex    pts/4       2023-12-16 21:59
test    tty3        2023-12-16 22:20
root@alex-nb -#
```

Рисунок 4 – Последний вход

```
-----
time-->Sat Dec 16 22:20:58 2023
type=PROCTITLE msg=audit(1702754458.309:23745): proctitle="(agetty)"
type=PATH msg=audit(1702754458.309:23745): item=0 name="/var/run/utmp" inode=1674 dev=00:17 mode=0100664 ouid=0 ogid=9
97 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=SYSCALL msg=audit(1702754458.309:23745): arch=c000003e syscall=257 success=yes exit=5 a0=ffffff9c a1=7fcc30b59f60
a2=800002 a3=0 items=1 ppid=1 pid=39785 auid=1001 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty3 ses
=16 comm="login" exe="/usr/bin/login" key="session"
-----
time-->Sat Dec 16 22:20:58 2023
type=PROCTITLE msg=audit(1702754458.309:23746): proctitle="(agetty)"
type=PATH msg=audit(1702754458.309:23746): item=0 name="/var/log/wtmp" inode=5505906 dev=103:06 mode=0100664 ouid=0 og
id=997 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=SYSCALL msg=audit(1702754458.309:23746): arch=c000003e syscall=257 success=yes exit=4 a0=ffffff9c a1=55e9763606f6
a2=800001 a3=0 items=1 ppid=1 pid=39785 auid=1001 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty3 ses
=16 comm="login" exe="/usr/bin/login" key="session"
```

Рисунок 5 – Логи аудита

## 2.3 Управление учётными записями

Для логирования административных действий подходит следующий раздел:

```
## User, group, password databases
-w /etc/group -p wa -k etcgroup
-w /etc/passwd -p wa -k etcpasswd
-w /etc/gshadow -k etcgroup
-w /etc/shadow -k etcpasswd
-w /etc/security/opasswd -k opasswd
```

```
## Tools to change group identifiers
-w /usr/sbin/groupadd -p x -k group_modification
-w /usr/sbin/groupmod -p x -k group_modification
-w /usr/sbin/addgroup -p x -k group_modification
-w /usr/sbin/useradd -p x -k user_modification
-w /usr/sbin/userdel -p x -k user_modification
-w /usr/sbin/usermod -p x -k user_modification
-w /usr/sbin/adduser -p x -k user_modification
```

## Листинг 2 – Управление учётными записями

Проверим создание и удаление пользователя по ключу `user_modification`. Создадим и удалим пользователя (рисунок 6). Соответствующие записи появились в логах аудита (рисунок 7).

```
root@alex-nb ~#
root@alex-nb ~# useradd -m test2
root@alex-nb ~# userdel test2
root@alex-nb ~# ausearch -k user_modification
```

## Рисунок 6 – Создание и удаление пользователя

```
-----
time->Sat Dec 16 23:47:38 2023
type=PROCTITLE msg=audit(1702759658.999:58612): proctitle=75736572616464002D6D007465737432
type=PATH msg=audit(1702759658.999:58612): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=134429 dev=103:06 mode=0100
755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702759658.999:58612): item=0 name="/usr/bin/useradd" inode=148036 dev=103:06 mode=0100755 ouid=0
ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1702759658.999:58612): argc=3 a0="useradd" a1="-m" a2="test2"
type=SYSCALL msg=audit(1702759658.999:58612): arch=c000003e syscall=59 success=yes exit=0 a0=55a160563500 a1=55a160566
0a0 a2=55a1603deb90 a3=8 items=2 ppid=38004 pid=45897 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="useradd" exe="/usr/bin/useradd" key="user_modification"
-----
time->Sat Dec 16 23:47:41 2023
type=PROCTITLE msg=audit(1702759661.546:58693): proctitle=7573657264656C007465737432
type=PATH msg=audit(1702759661.546:58693): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=134429 dev=103:06 mode=0100
755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702759661.546:58693): item=0 name="/usr/bin/userdel" inode=148037 dev=103:06 mode=0100755 ouid=0
ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1702759661.546:58693): argc=2 a0="userdel" a1="test2"
type=SYSCALL msg=audit(1702759661.546:58693): arch=c000003e syscall=59 success=yes exit=0 a0=55a16057cfc0 a1=55a160570
880 a2=55a160581780 a3=8 items=2 ppid=38004 pid=45908 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="userdel" exe="/usr/bin/userdel" key="user_modification"
root@alex-nb ~#
```

## Рисунок 7 – Логи аудита

## 2.4 Аудит изменения политики

Для логирования изменений в политику `auditd` подходит следующий раздел:

```
# 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 operating
-w /etc/audit/ -p wa -k auditconfig
-w /etc/libaudit.conf -p wa -k auditconfig
-w /etc/audit/ -p wa -k auditconfig

## 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/auditrules -p x -k audittools
```

### Листинг 3 – Аудит изменения политики

Выполним команду `auditctl` и проверим, появились ли логи (рисунки 8, 9).

```
root@alex-nb ~# auditctl -R /etc/audit/audit.rules
No rules
enabled 1
failure 1
pid 32110
```

Рисунок 8 – `auditctl`

```
-----
time->Sun Dec 17 00:12:42 2023
type=PROCTITLE msg=audit(1702761162.098:61843): proctitle=617564697463746C002D52002F6574632F61756469742F61756469742E72
756C6573
type=PATH msg=audit(1702761162.098:61843): item=0 name="/usr/sbin/" inode=131081 dev=103:06 mode=040755 ouid=0 ogid=0
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1702761162.098:61843): cwd="/root"
type=SOCKADDR msg=audit(1702761162.098:61843): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1702761162.098:61843): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffee72965a0 a2=4
3c a3=0 items=1 ppid=38004 pid=46821 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8
comm="auditctl" exe="/usr/bin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1702761162.098:61843): auid=1000 ses=8 op=add_rule key="audittools" list=4 res=1
-----
time->Sun Dec 17 00:12:42 2023
type=PROCTITLE msg=audit(1702761162.098:61844): proctitle=617564697463746C002D52002F6574632F61756469742F61756469742E72
756C6573
type=PATH msg=audit(1702761162.098:61844): item=0 name="/usr/sbin/" inode=131081 dev=103:06 mode=040755 ouid=0 ogid=0
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1702761162.098:61844): cwd="/root"
type=SOCKADDR msg=audit(1702761162.098:61844): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1702761162.098:61844): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffee72965a0 a2=4
3c a3=0 items=1 ppid=38004 pid=46821 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8
comm="auditctl" exe="/usr/bin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1702761162.098:61844): auid=1000 ses=8 op=add_rule key="audittools" list=4 res=1
-----
time->Sun Dec 17 00:12:42 2023
type=PROCTITLE msg=audit(1702761162.098:61845): proctitle=617564697463746C002D52002F6574632F61756469742F61756469742E72
756C6573
type=PATH msg=audit(1702761162.098:61845): item=0 name="/usr/sbin/" inode=131081 dev=103:06 mode=040755 ouid=0 ogid=0
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1702761162.098:61845): cwd="/root"
type=SOCKADDR msg=audit(1702761162.098:61845): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1702761162.098:61845): arch=c000003e syscall=44 success=yes exit=1088 a0=3 a1=7ffee72965a0 a2=4
40 a3=0 items=1 ppid=38004 pid=46821 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8
comm="auditctl" exe="/usr/bin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1702761162.098:61845): auid=1000 ses=8 op=add_rule key="audittools" list=4 res=1
-----
time->Sun Dec 17 00:12:42 2023
type=PROCTITLE msg=audit(1702761162.098:61846): proctitle=617564697463746C002D52002F6574632F61756469742F61756469742E72
756C6573
type=PATH msg=audit(1702761162.098:61846): item=0 name="/usr/sbin/" inode=131081 dev=103:06 mode=040755 ouid=0 ogid=0
rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1702761162.098:61846): cwd="/root"
type=SOCKADDR msg=audit(1702761162.098:61846): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1702761162.098:61846): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffee72965a0 a2=4
3c a3=0 items=1 ppid=38004 pid=46821 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8
comm="auditctl" exe="/usr/bin/auditctl" key=(null)
type=CONFIG_CHANGE msg=audit(1702761162.098:61846): auid=1000 ses=8 op=add_rule key="audittools" list=4 res=1
-----
time->Sun Dec 17 00:12:56 2023
type=PROCTITLE msg=audit(1702761176.265:62231): proctitle=6175736561726368002D68006175646974746F66C73
type=PATH msg=audit(1702761176.265:62231): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=134429 dev=103:06 mode=0100
755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702761176.265:62231): item=0 name="/usr/bin/ausearch" inode=144939 dev=103:06 mode=0100755 ouid=0
ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1702761176.265:62231): argc=3 a0="ausearch" a1="-k" a2="audittools"
type=SYSCALL msg=audit(1702761176.265:62231): arch=c000003e syscall=59 success=yes exit=0 a0=55a16056fe30 a1=55a16057f
c20 a2=55a16058a3d0 a3=8 items=2 ppid=38004 pid=46852 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="ausearch" exe="/usr/bin/ausearch" key="audittools"
root@alex-nb ~#
```

Рисунок 9 – Логи аудита

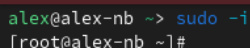
## 2.5 Аудит использования привилегий

Для логирования использования привилегий подходит следующий раздел:

```
## Process ID change (switching accounts) applications
-w /bin/su -p x -k priv_esc
-w /usr/bin/sudo -p x -k priv_esc
```

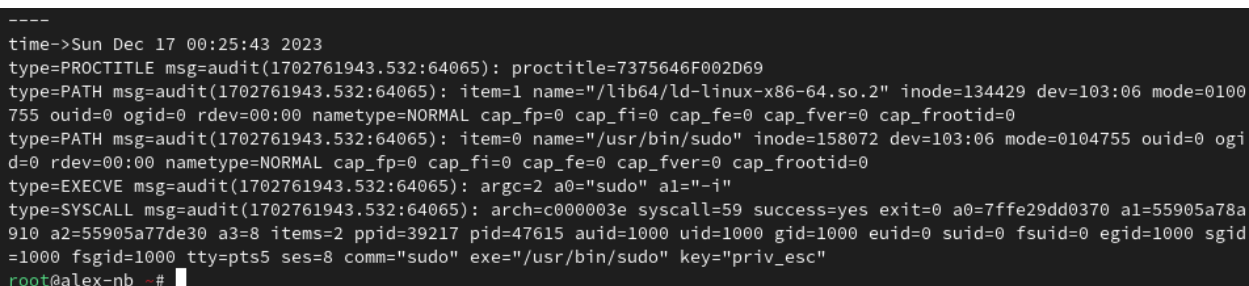
### Листинг 4 – Аудит использования привилегий

Выполним команду `sudo -i` и проверим, появились ли логи (рисунки 10, 11).



```
alex@alex-nb -> sudo -i
[root@alex-nb ~]#
```

Рисунок 10 – `sudo -i`



```
----
time->Sun Dec 17 00:25:43 2023
type=PROCTITLE msg=audit(1702761943.532:64065): proctitle=7375646F002D69
type=PATH msg=audit(1702761943.532:64065): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=134429 dev=103:06 mode=0100
755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702761943.532:64065): item=0 name="/usr/bin/sudo" inode=158072 dev=103:06 mode=0104755 ouid=0 ogi
d=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1702761943.532:64065): argc=2 a0="sudo" a1="-i"
type=SYSCALL msg=audit(1702761943.532:64065): arch=c000003e syscall=59 success=yes exit=0 a0=7ffe29dd0370 a1=55905a78a
910 a2=55905a77de30 a3=8 items=2 ppid=39217 pid=47615 auid=1000 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1000 sgid
=1000 fsgid=1000 tty=pts5 ses=8 comm="sudo" exe="/usr/bin/sudo" key="priv_esc"
root@alex-nb -#
```

Рисунок 11 – Логи аудита

## 2.6 Аудит доступа пользователя к объектам

Для логирования неудачных попыток пользователей получить доступ к разделам файловой системы подходит следующий фрагмент правил:

```
## 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 -F exit=-EACCES -F auid>=1000 -F auid!=--1 -k
file_access
-a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at
-S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=--1 -k
file_access

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

### Unsuccessful Modification
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S
setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES
-k file_modification
-a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S
setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k
file_modification
```

### Листинг 5 – Аудит доступа пользователя к объектам

Попробуем изменить файл `/etc/shadow` и проверим, появились ли логи об отказе в доступе (рисунки 10, 11).



```
alex@alex-nb ~ [1]> truncate /etc/shadow --size 0
truncate: cannot open '/etc/shadow' for writing: Permission denied
alex@alex-nb ~ [1]>
```

Рисунок 12 – truncate

```
-----
time-->Sun Dec 17 00:47:13 2023
type=PROCTITLE msg=audit(1702763233.672:72090): proctitle=7472756E63617465002F6574632F736861646F77002D2D73697A650030
type=PATH msg=audit(1702763233.672:72090): item=1 name="/etc/shadow" inode=4325561 dev=103:06 mode=0100600 ouid=0 ogid
=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702763233.672:72090): item=0 name="/etc/" inode=4325377 dev=103:06 mode=040755 ouid=0 ogid=0 rdev
=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=SYSCALL msg=audit(1702763233.672:72090): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7ffdb13b7a7
7 a2=841 a3=1b6 items=2 ppid=39217 pid=49391 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid
=1000 fsgid=1000 tty=pts5 ses=8 comm="truncate" exe="/usr/bin/truncate" key="file_access"
root@alex-nb /e/audit#
```

Рисунок 13 – Логи аудита

### 3 Выводы о проделанной работе

В ходе работы рассмотрены возможности, варианты применения и настройки системы audit, а также ее изначальные параметры. Получены знания о механизмах обеспечения безопасности ОС Linux, навыки настроек правил auditd, протоколирование важной с точки зрения безопасности информации.