

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Аудит

Отчет по лабораторной работе 3
по дисциплине «Информационная Безопасность»
студента 3 курса группы ИВТ-б-о-201(1)
Шор Константина Александровича

Направления подготовки 09.03.01 «Информатика и вычислительная техника»

Симферополь, 2023

ФСЭК №239

Условное обозначение и № меры	Меры защиты информации в ИС	Категория значимости КИИ		
		3	2	1
АУД.0	Разработка политики аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+

Условное обозначение и № меры	Меры защиты информации в ИС	Категория значимости КИИ		
		3	2	1
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+

Этапы



Должности

- Организатор внутреннего аудита ИБ организации (ОА)
- Руководитель проверяемого подразделения организации (РППО)
- Руководитель аудиторской группы (РАГ)
- Представители проверяемого подразделения организации (ПППО)
- Руководитель проверяющей организации (РПО)
- Сотрудники организации, предоставляющие источники свидетельств аудита ИБ (СППО)
- Аудиторы (эксперты) (А)
- Технические эксперты (ТЭ)

АЛГОРИТМ





ИНИЦИАЛИЗАЦИЯ

Systemd

/usr/lib/systemd – директория с юнитами по умолчанию

/etc/systemd – директория с управляемыми юнитами

ЖУРНАЛИРОВАНИЕ

Journald

Хранит данные:

- /run/log/journal
- /var/log/journal

Управляется:

Journalctl

Настройки:

/etc/systemd/journald.conf

0 — EMERG

1 — ALERT

2 — CRIT

3 — ERR

4 — WARNING

5 — NOTICE

6 — INFO

7 — DEBUG

```
(root@kali)~[/run/log/journal]
# systemctl status systemd-journald
● systemd-journald.service - Journal Service
   Loaded: loaded (/lib/systemd/system/systemd-journald.service; static)
   Active: active (running) since Sat 2023-01-07 05:36:05 EST; 2s ago
 TriggeredBy: ● systemd-journald-dev-log.socket
               ● systemd-journald.socket
               ● systemd-journald-audit.socket
   Docs: man:systemd-journald.service(8)
         man:journald.conf(5)
 Main PID: 23754 (systemd-journal)
   Status: "Processing requests ..."
    Tasks: 1 (limit: 2287)
  Memory: 1.2M
     CPU: 13ms
   CGroup: /system.slice/systemd-journald.service
           └─23754 /lib/systemd/systemd-journald

Jan 07 05:36:05 kali systemd-journald[23754]: Journal started
Jan 07 05:36:05 kali systemd-journald[23754]: System Journal (/var/log/journal/3095ed18a81a4f50ba21f01bf6332087) is 88.0M, max 4.0G, 3.9G free.
```

Auditd

Настройки

```
(root@kali)-[~]  
# cat /etc/audit/auditd.conf  
#  
# This file controls the configuration of the audit daemon  
#
```

```
#  
# This file controls the configuration of the audit daemon  
#  
  
local_events = yes  
write_logs = yes  
log_file = /var/log/audit/audit.log  
log_group = adm  
log_format = ENRICHED  
flush = INCREMENTAL_ASYNC  
freq = 50  
max_log_file = 8  
num_logs = 5  
priority_boost = 4  
name_format = NONE  
##name = mydomain  
max_log_file_action = ROTATE  
space_left = 75  
space_left_action = SYSLOG  
verify_email = yes  
action_mail_acct = root  
admin_space_left = 50  
admin_space_left_action = SUSPEND  
disk_full_action = SUSPEND  
disk_error_action = SUSPEND  
use_libwrap = yes  
##tcp_listen_port = 60  
tcp_listen_queue = 5  
tcp_max_per_addr = 1  
##tcp_client_ports = 1024-65535  
tcp_client_max_idle = 0  
transport = TCP  
krb5_principal = auditd  
##krb5_key_file = /etc/audit/audit.key  
distribute_network = no  
q_depth = 1200  
overflow_action = SYSLOG  
max_restarts = 10  
plugin_dir = /etc/audit/plugins.d  
end_of_event_timeout = 2
```


Правила

```
(root@kali)-[/etc/audit]
# cat audit.rules
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000
```

Состояние

```
(root@kali)-[/etc/audit/rules.d]
# auditctl -s
enabled 1
failure 1
pid 4906
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
loginuid_immutable 0 unlocked
```

Автозагрузка сервиса

```
(root@kali)-[~]
# systemctl status auditd
o auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
```

```
(root@kali)-[/etc/audit/rules.d]
# systemctl enable auditd.service
Synchronizing state of auditd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable auditd
Created symlink /etc/systemd/system/multi-user.target.wants/auditd.service → /lib/systemd/system/auditd.service.
```

```

# systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; preset: disabled)
   Active: active (running) since Wed 2023-01-11 03:25:07 EST; 27s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 363 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Process: 473 ExecStartPost=/sbin/auditd --load (code=exited, status=0/SUCCESS)
   Main PID: 467 (auditd)
      Tasks: 2 (limit: 2287)
     Memory: 5.2M
        CPU: 101ms
    CGroup: /system.slice/auditd.service
           └─467 /sbin/auditd

```

1. Определите какие системные демоны для аудита имеются в вашей системе — какие осуществляют функции syslogd, klogd, а какие аналогичны auditd. Изучите документацию по ним.

```

(root@kali)-[/home/kali]
# klogd
Command 'klogd' not found, but can be installed with:
apt install busybox-syslogd
Do you want to install it? (N/y)y
apt install busybox-syslogd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gnome-bluetooth-common libgnome-bluetooth13
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  busybox
The following NEW packages will be installed:
  busybox-syslogd
The following packages will be upgraded:
  busybox
1 upgraded, 1 newly installed, 0 to remove and 813 not upgraded.
Need to get 7,928 B/460 kB of archives.
After this operation, 46.1 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 busybox-syslogd all 1:1.35.0-4 [7,928 B]
Fetched 7,928 B in 2s (4,648 B/s)
(Reading database ... 418932 files and directories currently installed.)
Preparing to unpack .../busybox_1%3a1.35.0-4+b1_amd64.deb ...
Unpacking busybox (1:1.35.0-4+b1) over (1:1.35.0-4) ...
Selecting previously unselected package busybox-syslogd.
Preparing to unpack .../busybox-syslogd_1%3a1.35.0-4_all.deb ...
Unpacking busybox-syslogd (1:1.35.0-4) ...
Setting up busybox (1:1.35.0-4+b1) ...
Setting up busybox-syslogd (1:1.35.0-4) ...
update-rc.d: We have no instructions for the busybox-syslogd init script.
update-rc.d: It looks like a non-network service, we enable it.
update-rc.d: We have no instructions for the busybox-klogd init script.
update-rc.d: It looks like a non-network service, we enable it.
Processing triggers for initramfs-tools (0.142) ...
update-initramfs: Generating /boot/initrd.img-6.0.0-kali3-amd64
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...

```

```

(root@kali)-[/home/kali]
# systemctl status syslogd
● busybox-syslogd.service - LSB: Starts syslogd
   Loaded: loaded (/etc/init.d/busybox-syslogd; generated)
   Active: active (running) since Sun 2023-01-08 04:20:24 EST; 13min ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 2287)
   Memory: 448.0K
      CPU: 19ms
   CGroup: /system.slice/busybox-syslogd.service
           └─2518 /sbin/syslogd -C128

Jan 08 04:20:24 kali systemd[1]: Starting LSB: Starts syslogd...
Jan 08 04:20:24 kali busybox-syslogd[2511]: Starting busybox' syslogd implementation : syslogd
Jan 08 04:20:24 kali busybox-syslogd[2520]: 2518 (syslogd)
Jan 08 04:20:24 kali busybox-syslogd[2511]: .
Jan 08 04:20:24 kali systemd[1]: Started LSB: Starts syslogd.

(root@kali)-[/home/kali]
# systemctl status klogd
● busybox-klogd.service - LSB: Starts klogd
   Loaded: loaded (/etc/init.d/busybox-klogd; generated)
   Active: active (exited) since Sun 2023-01-08 04:20:24 EST; 13min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 2558 ExecStart=/etc/init.d/busybox-klogd start (code=exited, status=0/SUCCESS)
     CPU: 1ms

Jan 08 04:20:24 kali systemd[1]: Starting LSB: Starts klogd...
Jan 08 04:20:24 kali systemd[1]: Started LSB: Starts klogd.

```

- Создайте 3-4 пользователя в системе и установите им разные уровни доступа к запуску определенных программ, чтению каких-либо текстовых файлов и записи в какой-то файл с данными (все необходимые файлы создайте, если их нет).

```

(root@kali)-[~user_1/test_file]
# ls -l
total 28
-rw-r--rw- 1 root root 296 Jan 7 14:51 admin_message.txt
-rw----- 1 user_1 user_1 9 Jan 7 14:51 passwd_1.txt
-rw----- 1 user_2 user_2 9 Jan 7 14:51 passwd_2.txt
-rw----- 1 user_3 user_3 9 Jan 7 14:51 passwd_3.txt
-rwxr----- 1 user_1 root 38 Jan 7 14:51 script_1
-rwxr----- 1 user_2 root 38 Jan 7 14:51 script_2
-rwxr----- 1 user_3 root 38 Jan 7 14:51 script_3

```


3. Проведите сеансы работы от имени каждого пользователя с полным перечнем попыток доступа всех типов ко всем объектам
4. Прочитайте журналы системного аудита и аудита безопасности, которые получились в результате работы с настройками по умолчанию.

User_1

```
(root@kali)-[~/user_1/test_file]
# su user_1
(user_1@kali)-[~/test_file]
$ ls
admin_message.txt  passwd_1.txt  passwd_2.txt  passwd_3.txt  script_1  script_2  script_3

(user_1@kali)-[~/test_file]
$ nano admin_message.txt

(user_1@kali)-[~/test_file]
$ nano passwd_1.txt

(user_1@kali)-[~/test_file]
$ nano passwd_2.txt

(user_1@kali)-[~/test_file]
$ nano passwd_3.txt

(user_1@kali)-[~/test_file]
$ ./script_1

Broadcast message from user_1@kali (pts/3) (Sun Jan  8 08:18:25 2023):
Hello from user_1

● systemd-rfkill.socket - Load/Save RF Kill Switch Status /dev/rfkill Watch
   Loaded: loaded (/lib/systemd/system/systemd-rfkill.socket; static)
   Active: active (listening) since Sun 2023-01-08 08:18:29 EST; 12ms ago
   Until: Sun 2023-01-08 08:18:29 EST; 12ms ago
   Triggers: ● systemd-rfkill.service
   Docs: man:systemd-rfkill.socket(8)
   Listen: /dev/rfkill (Special)
   CGroup: /system.slice/systemd-rfkill.socket

Broadcast message from user_1@kali (pts/3) (Sun Jan  8 08:18:29 2023):
Ooops UwU

(user_1@kali)-[~/test_file]
$ exit

(root@kali)-[~/user_1/test_file]
#
```

```
Jan 08 08:17:36 kali audit[34816]: (to user_1) root on pts/3
Jan 08 08:17:36 kali audit[34816]: USER_ACCT pid=34816 uid=0 auid=1000 ses=2 subj=unconfined msg='op-PAM:authentication grantors=pam_permit acct='user_1' exe='/usr/bin/su' hostname=? addr=? terminal=/dev/pts/3 res=success'
Jan 08 08:17:36 kali audit[34816]: CRED_ACQ pid=34816 uid=0 auid=1000 ses=2 subj=unconfined msg='op-PAM:setcred grantors=pam_rootok acct='user_1' exe='/usr/bin/su' hostname=? addr=? terminal=/dev/pts/3 res=success'
Jan 08 08:17:36 kali audit[34816]: pam_unix(su:session): session opened for user user_1(uid=1001) by kali(uid=0)
Jan 08 08:17:36 kali audit[34816]: USER_START pid=34816 uid=0 auid=1000 ses=2 subj=unconfined msg='op-PAM:session.open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct='user_1' exe='/usr/bin/su' hostname=? addr=? terminal=/dev/pts/3 res=success'

Broadcast message from user_1@kali (pts/3) (Sun Jan  8 08:18:25 2023):
Hello from user_1

Jan 08 08:18:25 kali polkitd[470]: Registered Authentication Agent for unix-process:35091:76727 (system bus name :1.170 [/usr/bin/pktyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)

Broadcast message from user_1@kali (pts/3) (Sun Jan  8 08:18:29 2023):
Ooops UwU

Jan 08 08:18:29 kali audit[35104]: USER_AUTH pid=35104 uid=1000 auid=1000 ses=2 subj=unconfined msg='op-PAM:authentication grantors=pam_permit acct='kali' exe='/usr/lib/polkit-1/polkit-agent-helper-1' hostname=? addr=? terminal=? res=success'
Jan 08 08:18:29 kali audit[35104]: USER_ACCT pid=35104 uid=1000 auid=1000 ses=2 subj=unconfined msg='op-PAM:setcred grantors=pam_rootok acct='kali' exe='/usr/lib/polkit-1/polkit-agent-helper-1' hostname=? addr=? terminal=? res=success'
Jan 08 08:18:29 kali polkitd[470]: Operator of unix-session:2 successfully authenticated as unix-user:kali to gain TEMPORARY authorization for action org.freedesktop.systemd1.manage-units for system-bus-name=:1.171 [systemctl start systemd-rfkill.socket] (owned by unix-user:zer-2)
Jan 08 08:18:29 kali systemd[1]: Listening on Load/Save RF Kill Switch Status /dev/rfkill Watch.
Jan 08 08:18:29 kali polkitd[470]: Unregistered Authentication Agent for unix-process:35091:76727 (system bus name :1.170, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 08 08:18:25 kali audit[34816]: pam_unix(su:session): session closed for user user_1
Jan 08 08:18:35 kali audit[34816]: USER_END pid=34816 uid=0 auid=1000 ses=2 subj=unconfined msg='op-PAM:session.close grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct='user_1' exe='/usr/bin/su' hostname=? addr=? terminal=/dev/pts/3 res=success'
Jan 08 08:18:35 kali audit[34816]: CRED_RELEASE pid=34816 uid=0 auid=1000 ses=2 subj=unconfined msg='op-PAM:setcred grantors=pam_rootok acct='user_1' exe='/usr/bin/su' hostname=? addr=? terminal=/dev/pts/3 res=success'
```

User_2

```
(root@kali)-[~user_1/test_file]
# su user_2
(user_2@kali)-[/home/user_1/test_file]
$ ls
admin_message.txt  passwd_1.txt  passwd_2.txt  passwd_3.txt  script_1  script_2  script_3
(user_2@kali)-[/home/user_1/test_file]
$ nano admin_message.txt
(user_2@kali)-[/home/user_1/test_file]
$ nano passwd_1.txt
(user_2@kali)-[/home/user_1/test_file]
$ nano passwd_2.txt
(user_2@kali)-[/home/user_1/test_file]
$ nano passwd_3.txt
(user_2@kali)-[/home/user_1/test_file]
$ ./script_2

Broadcast message from user_2@kali (pts/3) (Sun Jan  8 08:28:53 2023):

Hello from user_2

Jan  8 08:28:56 kali audit[37722]:
Broadcast message from user_2@kali (pts/3) (Sun Jan  8 08:28:56 2023):

Oooouups UwU

Jan  8 08:28:56 kali polkitd[470]: Operator of unix-session:2 successfully authenticated a
md-rfkill.socket] (owned by unix-user:user_2)
(user_2@kali)-[/home/user_1/test_file]
$ exit

Jan  8 08:28:56 kali systemd[1]: Closed Load/Save RF Kill Switch Status /dev/rfkill Watch.
Jan  8 08:28:56 kali polkitd[470]: Unregistered Authentication Agent for unix-process:3770
#
(root@kali)-[~user_1/test_file]
#
```

```
Jan 08 08:27:55 kali su[37374]: (to user_2) root on pts/3
Jan 08 08:27:55 kali audit[37374]: USER_ACCT pid=37374 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:accounting grantors=pam_permit acct="user_2" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:27:55 kali audit[37374]: CRED_ACQ pid=37374 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:setcred grantors=pam_rootok acct="user_2" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:27:55 kali su[37374]: pam_unix(su:session): session opened for user user_2(uid=1002) by kali(uid=0)
Jan 08 08:27:55 kali audit[37374]: USER_START pid=37374 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:session_open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct="user_2" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success

Broadcast message from user_2@kali (pts/3) (Sun Jan  8 08:28:53 2023):

Hello from user_2

Jan 08 08:28:53 kali polkitd[470]: Registered Authentication Agent for unix-process:37709:830109 (system bus name :1.175 [/usr/bin/pktyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)

Broadcast message from user_2@kali (pts/3) (Sun Jan  8 08:28:56 2023):

Oooouups UwU

Jan 08 08:28:56 kali audit[37722]: USER_AUTH pid=37722 uid=1000 auid=1000 ses=2 subj=unconfined msg=op-PAM:authentication grantors=pam_permit acct="kali" exe="/usr/lib/polkit-1/polkit-agent-helper-1" hostname=? addr=? terminal=? res=success
Jan 08 08:28:56 kali audit[37722]: USER_ACCT pid=37722 uid=1000 auid=1000 ses=2 subj=unconfined msg=op-PAM:accounting grantors=pam_permit acct="kali" exe="/usr/lib/polkit-1/polkit-agent-helper-1" hostname=? addr=? terminal=? res=success
Jan 08 08:28:56 kali polkitd[470]: Operator of unix-session:2 successfully authenticated as unix-user:kali to gain TEMPORARY authorization for action org.freedesktop.systemd1.manage-units for system-bus-name::1.176 [systemctl stop syste
md-rfkill.socket] (owned by unix-user:user_2)
Jan 08 08:28:56 kali systemd[1]: system-rfkill.socket: Deactivated successfully.
Jan 08 08:28:56 kali systemd[1]: Closed Load/Save RF Kill Switch Status /dev/rfkill Watch.
Jan 08 08:28:56 kali polkitd[470]: Unregistered Authentication Agent for unix-process:37709:830109 (system bus name :1.175, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 08 08:28:56 kali su[37374]: pam_unix(su:session): session closed for user user_2
Jan 08 08:28:56 kali audit[37374]: USER_END pid=37374 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:session_close grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct="user_2" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:28:56 kali audit[37374]: CRED_DISP pid=37374 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:setcred grantors=pam_rootok acct="user_2" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
```


User_3

```
(root@kali)-[~user_1/test_file] Stopping OpenBSD Secure Shell server...
# su user_3
(user_3@kali)-[/home/user_1/test_file]
$ ls
admin_message.txt  passwd_1.txt  passwd_2.txt  passwd_3.txt  script_1  script_2  script_3
Unregistered Authentication Agent for unix-process:41480:9184 (uid=0): session opened for user user_3
(user_3@kali)-[/home/user_1/test_file]
$ nano admin_message.txt
(user_3@kali)-[/home/user_1/test_file]
$ nano passwd_1.txt
(user_3@kali)-[/home/user_1/test_file] (to user_3) root on pts/3
$ nano passwd_2.txt
(user_3@kali)-[/home/user_1/test_file]
$ nano passwd_3.txt
(user_3@kali)-[/home/user_1/test_file] (Sun Jan  8 08:43:41 2023):
$ ./script_3

Broadcast message from user_3@kali (pts/3) (Sun Jan  8 08:43:41 2023):
Hello from user_3

o ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: inactive (dead) since Sun 2023-01-08 08:43:44 EST; 12ms ago
   Duration: 1min 5.905s
   Docs: man:sshd(8)
        man:sshd_config(5)
   Process: 41502 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Process: 41503 ExecStart=/usr/sbin/sshd -D $SSH_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 41503 (code=exited, status=0/SUCCESS)
   CPU: 24ms
Unregistered Authentication Agent for unix-process:41858:9184 (uid=0): session opened for user user_3
$ exit
(root@kali)-[~user_1/test_file]
```

```
Jan 08 08:42:59 kali su[41013]: (to user_3) root on pts/3
Jan 08 08:42:59 kali audit[41013]: USER_ACCT pid=41013 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:accounting grantors=pam_permit acct="user_3" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:42:59 kali audit[41013]: CMO_ACG pid=41013 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:session_open grantors=pam_rootok acct="user_3" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:42:59 kali su[41013]: pam_unix(su:session): session opened for user user_3(uid=1003) by kali(uid=0)
Jan 08 08:42:59 kali audit[41013]: USER_START pid=41013 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:session_open grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct="user_3" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success

Broadcast message from user_3@kali (pts/3) (Sun Jan  8 08:43:41 2023):
Hello from user_3

Jan 08 08:43:41 kali polkitd[470]: Registered Authentication Agent for unix-process:41858:918909 (system bus name :1.206 [/usr/bin/pktyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jan 08 08:43:44 kali audit[41871]: USER_AUTH pid=41871 uid=1000 auid=1000 ses=2 subj=unconfined msg=op-PAM:authentication grantors=pam_permit acct="kali" exe="/usr/lib/polkit-1/polkit-agent-helper-1" hostname=? addr=? terminal=? res=success
Jan 08 08:43:44 kali audit[41871]: USER_ACCT pid=41871 uid=1000 auid=1000 ses=2 subj=unconfined msg=op-PAM:accounting grantors=pam_permit acct="kali" exe="/usr/lib/polkit-1/polkit-agent-helper-1" hostname=? addr=? terminal=? res=success
Jan 08 08:43:44 kali polkitd[470]: Operator of unix-session:2 successfully authenticated as unix-user:kali to gain TEMPORARY authorization for action org.freedesktop.systemd1.manage-units for system-bus-name=:1.207 [systemctl stop ssh] (owned by unix-user:user_3)
Jan 08 08:43:44 kali systemd[1]: Stopping OpenBSD Secure Shell server...
Jan 08 08:43:44 kali sshd[41503]: Received signal 15; terminating.
Jan 08 08:43:44 kali systemd[1]: ssh.service: Deactivated successfully.
Jan 08 08:43:44 kali systemd[1]: Stopped OpenBSD Secure Shell server.
Jan 08 08:43:44 kali audit[1]: SERVICE_STOP pid=1 uid=0 auid=0 ses=0 subj=unconfined msg=unit-ssh comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
Jan 08 08:43:44 kali polkitd[470]: Unregistered Authentication Agent for unix-process:41858:918909 (system bus name :1.206, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 08 08:43:56 kali su[41013]: pam_unix(su:session): session closed for user user_3
Jan 08 08:43:56 kali audit[41013]: USER_END pid=41013 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:session_close grantors=pam_env,pam_env,pam_mail,pam_limits,pam_permit,pam_unix,pam_systemd acct="user_3" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
Jan 08 08:43:56 kali audit[41013]: CMO_DOSP pid=41013 uid=0 auid=1000 ses=2 subj=unconfined msg=op-PAM:setcred grantors=pam_rootok acct="user_3" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/3 res=success
```


5. Напишите конфигурацию демона auditd так, чтобы в журнал записывались только события доступа от двух пользователей при попытке их записи в файл данных или запуска программы, доступа к которым у них нет

-s – номер процесса

-w – файл

-F uid – пользователь

-k – ключ, по которому можно найти лог

```
(root@kali)-[/etc/audit/rules.d]
# auditctl -S 1 -w /home/user_1/test_file/passwd_2.txt -F uid=1001 -k beck_user_1

(root@kali)-[/etc/audit/rules.d]
# auditctl -S 59 -w /home/user_1/test_file/script_2 -F uid=1001 -k beck_user_1
```

auditctl -S 1 -w /home/user_1/test_file/passwd_2.txt -F uid=1001 -k beck_user_1

auditctl -S 59 -w /home/user_1/test_file/script_2 -F uid=1001 -k beck_user_1

```
(root@kali)-[/etc/audit/rules.d]
# auditctl -S 1 -w /home/user_1/test_file/passwd_1.txt -F uid=1002 -k beck_user_2

(root@kali)-[/etc/audit/rules.d]
# auditctl -S 59 -w /home/user_1/test_file/script_1 -F uid=1002 -k beck_user_2
```

auditctl -S 1 -w /home/user_1/test_file/passwd_1.txt -F uid=1002 -k beck_user_2

auditctl -S 59 -w /home/user_1/test_file/script_1 -F uid=1002 -k beck_user_2

Результат

Поиск по ключу

```
ausearch -k beck_user_1
```

[illegible]

```
ausearch -k beck_user_2
```

```
time=Sun Jan 8 12:02:11 2023
type=PROCTITLE msg-audit(167319731.4221752): prctitle=(c175646f7463c80d2530833908207802f686f60652f7536572f312746573f5f6696c652f736726970f45f13002d46007596e04b13380320020600626563085f7536572f5f32)
type=CMD msg-audit(167319731.4221752): cmd=/usr/bin/lsh -l -i /etc/passwd uid=0:0 mode=040755 oids=0:gid=0 rdev=0:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_footid=0
type=SCOCADIR msg-audit(167319731.4221752): saddr=1000000000000000000000000000000000
type=SYSCALL msg-audit(167319731.4221752): arch=x86_64 syscall=44 success=yes exit=-1100 a0=a4 i1=7ffc24394100 a2=a4c a3=a3 items1 ppid=76791 pid=90918 audit-1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=2 c0=0 audit1="" exe="/usr/sbin/auditctl" subj=unconfined key=[null]
type=CONFIG_CHANGE msg-audit(167319731.4221752): audit-1000 ses=2 subj=unconfined op=add_rule key="back_user_2" l1st=4 res=1

time=Sun Jan 8 12:03:34 2023
type=PROCTITLE msg-audit(1673197416.880753): prctitle=(c36174007861737376A5F312E747874)
type=PATH msg-audit(1673197416.880753): item#0 name=password,l1st="" inode=353941 dev=0:01 mode=010600 oid=1001 lgid=0:000 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_footid=0
type=CMD msg-audit(1673197416.880753): cmd=/home/user/.ltest.txt
type=SYSCALL msg-audit(1673197416.880753): arch=x86_64 syscall=1257 success=no exit=-13 a1=ffffffffff a17ff6fdb032 a2=a3 a3=0 items1 ppid=90019 pid=12153 audit-1002 uid=1002 gid=1002 fsuid=1002 euid=1002 sgid=1002 fsgid=1002 tty=pts3 ses=2 comm="cat" exe="/usr/bin/cat" subj=unconfined key="back_user_2"

time=Sun Jan 8 12:03:42 2023
type=PROCTITLE msg-audit(1673197422.239754): prctitle="(zsh)"
type=PATH msg-audit(1673197422.239754): item#0 name=.script,l1st="" inode=353941 dev=0:01 mode=0100740 uid=1001 lgid=0:000 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_footid=0
type=CMD msg-audit(1673197422.239754): cmd=/usr/bin/zsh --rcfile /etc/zshrc
type=SYSCALL msg-audit(1673197422.239754): arch=x86_64 syscall=59 success=no exit=-13 a0=7fad3935840 a1=7fad3935890 a2=56444db25980 a3=8 items1 ppid=90019 pid=91294 audit-1000 uid=1002 gid=1002 euid=1002 fsuid=1002 egid=1002 fsgid=1002 tty=pts5 ses=2 comm="zsh" exe="/usr/bin/zsh" subj=unconfined key="back_user_2"

root@kali: [/etc/audit/rules.d]
```