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	+	+	+

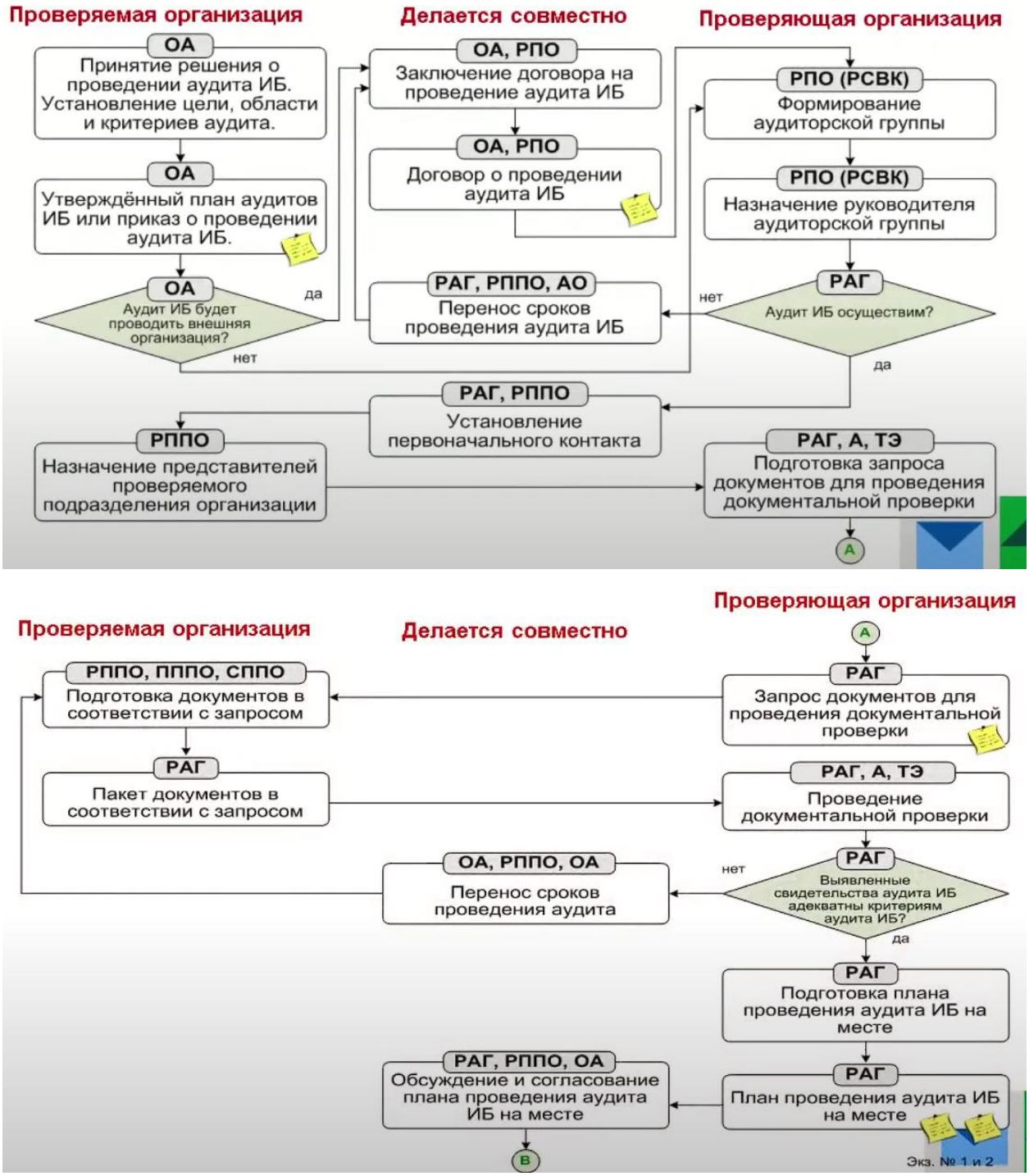
Условное обозначение и № меры	Меры защиты информации в ИС	Категория значимости КИИ		
		3	2	1
АУД.7	**Мониторинг безопасности**	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	**Проведение внутренних аудитов**	+	+	+
АУД.11	**Проведение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

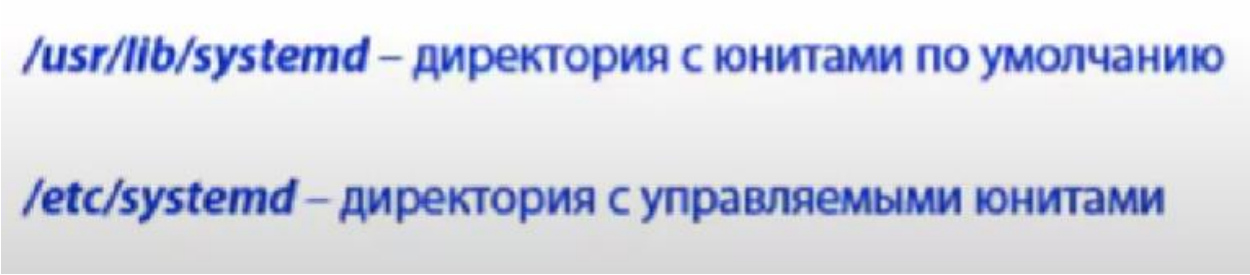

Проверяемая организация
Делается совместно
Проверяющая организация
ОА
Принятие решения о проведении аудита ИБ. Установление цели, области и критериев аудита.
ОА, РПО
Заключение договора на проведение аудита ИБ
РПО (РСВК)
Формирование аудиторской группы
ОА
Утверждённый план аудитов ИБ или приказ о проведении аудита ИБ.
ОА, РПО
Договор о проведении аудита ИБ
РПО (РСВК)
Назначение руководителя аудиторской группы
ОА
Аудит ИБ будет проводить внешняя организация?
да
нет
РАГ, РППО, АО
Перенос сроков проведения аудита ИБ
нет
РАГ
Аудит ИБ осуществим?
да
РАГ, РППО
Установление первоначального контакта
РППО
Назначение представителей проверяемого подразделения организации
РАГ, А, ТЭ
Подготовка запроса документов для проведения документальной проверки
A
Проверяющая организация
Проверяемая организация
Делается совместно
A
РППО, ППО, СППО
Подготовка документов в соответствии с запросом
РАГ
Запрос документов для проведения документальной проверки
РАГ
Пакет документов в соответствии с запросом
РАГ, А, ТЭ
Проведение документальной проверки
ОА, РППО, ОА
Перенос сроков проведения аудита
нет
РАГ
Выявленные свидетельства аудита ИБ адекватны критериям аудита ИБ?
да
РАГ
Подготовка плана проведения аудита ИБ на месте
РАГ, РППО, ОА
Обсуждение и согласование плана проведения аудита ИБ на месте
РАГ
План проведения аудита ИБ на месте
B
Экз. № 1 и 2


Проверяющая организация
Проверяемая организация
Делается совместно
B
РАГ
Распределение обязанностей между членами аудиторской группы
Протокол заседания
А
Подготовка документов для регистрации результатов аудита
РАГ, РППО, ППО, СППО
Проведение вступительного совещания
РАГ, А, ТЭ, РППО, ППО, СППО
Сбор свидетельств аудита ИБ при проведении аудита ИБ на месте
РАГ, А
Оценивание собранных свидетельств аудита ИБ и формирование выводов аудита ИБ
РАГ, А
Выводы аудита
РАГ, РППО
Согласование полученных выводов аудита ИБ
Шаблоны, бланки, опросные листы
Вывода аудита ИБ согласованы?
да
нет
РАГ, А
Подготовка заключения по результатам аудита ИБ
РАГ, А
Заключение по результатам аудита ИБ
РАГ, РППО
Регистрация нерешённых вопросов
C


Проверяемая организация
Делается совместно
Проверяющая организация (СВК)
РАГ, ОА, РППО
Проведение заключительного совещания с целью обсуждения выводов и заключения по результатам аудита ИБ
B
Выводы и заключения согласованы?
да
нет
РАГ, А
Подготовка отчёта по результатам проведения аудита ИБ
РАГ, РППО
Регистрация нерешённых вопросов
РАГ, А
Отчёт по результатам проведения аудита ИБ
РПО (РСВК), ОА
Сдача отчёта и заключения по результатам аудита ИБ

ИНИЦИАЛИЗАЦИЯ

Systemd



ЖУРНАЛИРОВАНИЕ

Journald


```
┌──(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
○ 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/augenrules --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) ...
```

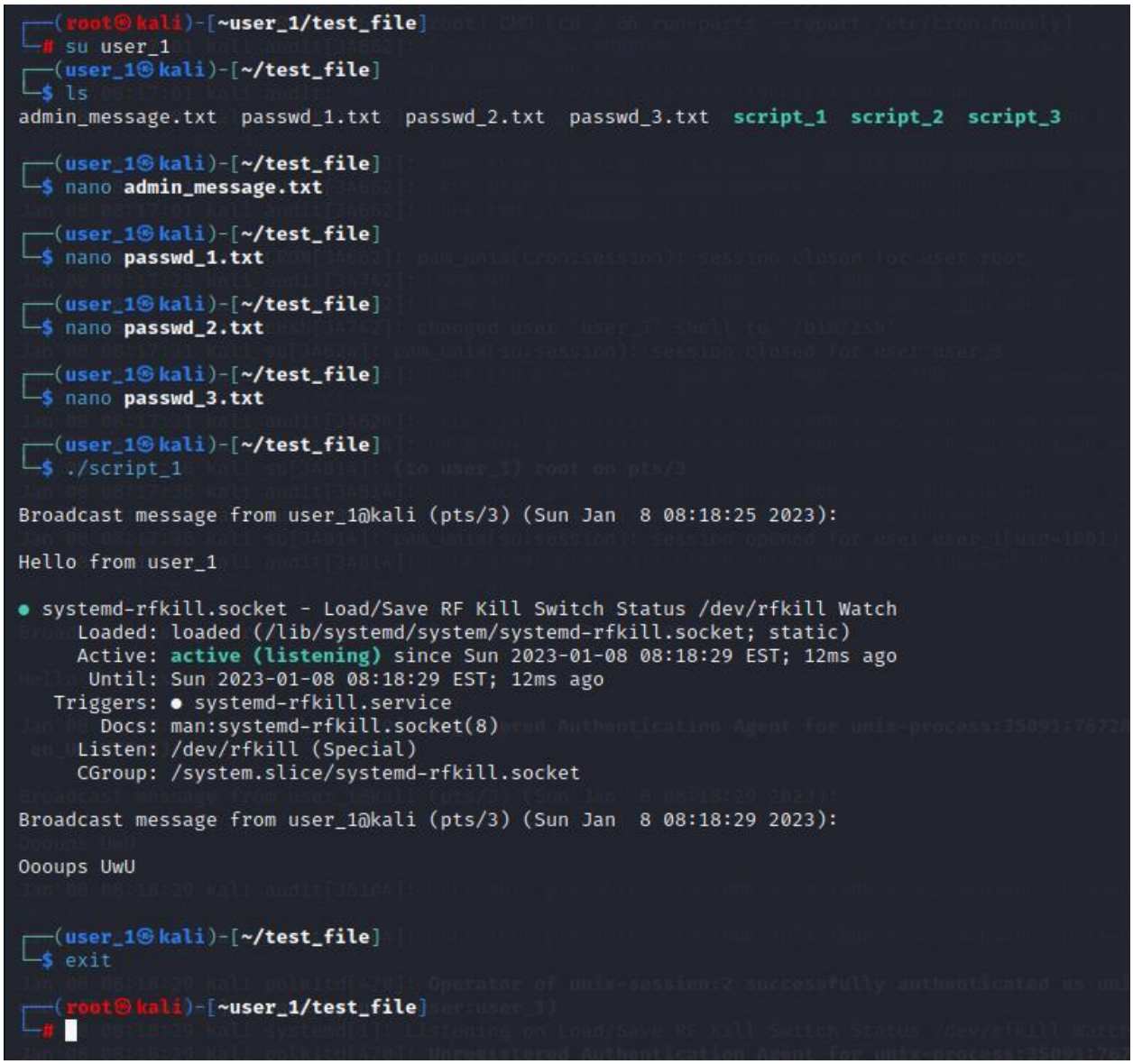
```
┌──(root㉿kali)-[/home/kali]
└─# systemctl status syslogd
● busybox-syslogd.service - LSB: Starts syslogd
     Loaded: loaded (/etc/init.d/busybox-syslogd; generated)
     Active: active (running) since Sun 2023-01-08 04:20:24 EST; 13min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 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.
```

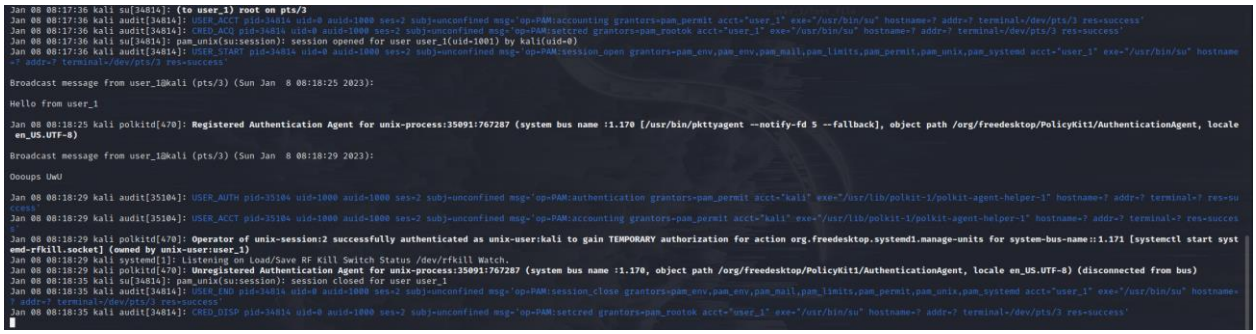
2. Создайте 3-4 пользователя в системе и установите им разные уровни доступа к запуску определенных программ, чтению каких-либо текстовых файлов и записи в какой-то файл с данными (все необходимые файлы создайте, если их нет).

```
┌──(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.

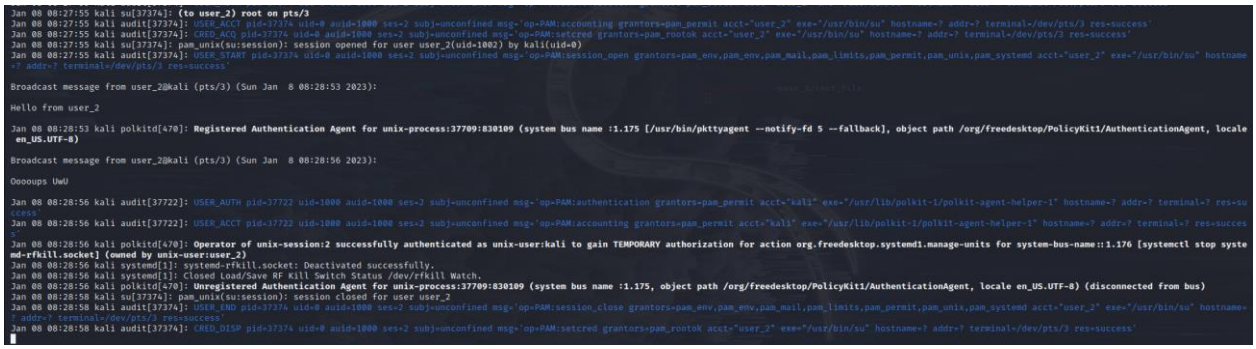
User_1





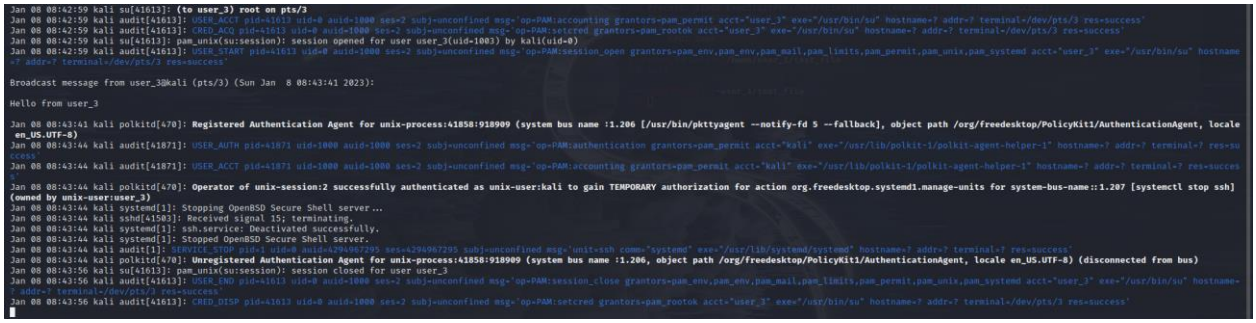
User_2

```
┌──(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


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

Oooooups UwU

┌──(user_2㉿kali)-[/home/user_1/test_file]
└─$ exit

┌──(root㉿kali)-[~user_1/test_file]
└─#
```



User_3

```
┌──(root㉿kali)-[~user_1/test_file]
└─# 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

┌──(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]
└─$ nano passwd_2.txt

┌──(user_3㉿kali)-[/home/user_1/test_file]
└─$ nano passwd_3.txt

┌──(user_3㉿kali)-[/home/user_1/test_file]
└─$ ./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 $SSHD_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 41503 (code=exited, status=0/SUCCESS)
        CPU: 24ms

┌──(user_3㉿kali)-[/home/user_1/test_file]
└─$ exit

┌──(root㉿kali)-[~user_1/test_file]
└─#
```



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
```

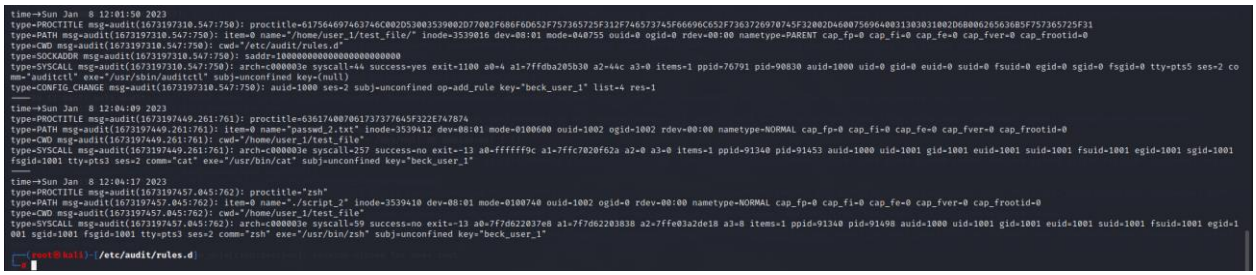
auditctl -S 1 -w /home/user_1/test_file/passwd_1.txt -F uid=1002 -k beck_user_2

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



ausearch -k beck_user_2