

Запустите виртуальную машину Exam-2022.

Используйте логин **ИБСТ** и пароль **ИБст123** для входа в систему.

Ответьте на вопросы последующих тестов

№1 – ПКМ на Мой компьютер -> Управление -> Локальные пользователи и группы -> Пользователи

Вопрос **1**

Выполнен

Баллов: 1,00 из 1,00

Отметить вопрос

Перечислите найденных пользователей в порядке алфавита. Отключенные учетные записи не учитывать. Учетную запись, под которой авторизовались в системе тоже не учитывать.

1.

Drobyn a

2.

Ivanov

3.

Lemzyaikin

4.

Levsky

5.

Mochkasov

6.

Nevsky

7.

Ogulo

8.

Petrov

9.

Shemysheikin

10.

Sheptalo

11.

Sidorov

№2 – ПКМ на Мой компьютер -> Управление -> Локальные пользователи и группы -> Группы:
смотрим группу и отмечаем членов

Выполнен

Баллов: 1,00 из 1,00

Отметить вопрос

Отметьте пользователей, входящих в группу
"Опытные пользователи"

Выберите один или несколько ответов:

- ☐ Pechatkin
- ☒ Mochkasov
- ☐ Semyonov
- ☐ Администратор
- ☐ Ogulo
- ☐ Nevsky
- ☐ Ivanov
- ☐ Borisov
- ☐ Sheptalo
- ☐ Ruzaykin
- ☐ Drobyna
- ☒ Lemzyaikin
- ☐ Levsky
- ☒ Shemysheikin
- ☐ Sidorov



№3 и №4:

В поисковой строке пишем eventvwr

Журналы Windows -> Безопасность -> Фильтр текущего журнала -> XML -> Изменить запрос вручную:

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">
      * [System[ (EventID=4624) ] ]
      and
      * [EventData[Data[@Name='TargetUserName'] and (Data='Петров') ] ]
    </Select>
  </Query>
</QueryList>
```

4624 - Успешный вход в систему

4625 - Отказ входа в систему

<p>Вопрос 3</p> <p>Выполнен</p> <p>Баллов: 2,00 из 2,00</p> <p>🚩 Отметить вопрос</p>	<p>Вопрос 4</p> <p>Выполнен</p> <p>Баллов: 2,00 из 2,00</p> <p>🚩 Отметить вопрос</p>
<p>Для пользователя Lemzyaikin определите:</p> <p>время последнего удачного входа в систему</p> <p>12.05.2017 16:43:52</p> <p>время последней неудачной аутентификации</p> <p>30.12.2021 12:37:40</p> <p>Время вводите в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС</p> <p>Между датой и временем должен быть только один пробел. Пробелов перед датой и после времени быть не должно.</p>	<p>Для пользователя Petrov определите:</p> <p>время последнего удачного входа в систему</p> <p>12.05.2017 16:14:34</p> <p>время последней неудачной аутентификации</p> <p>30.12.2021 12:38:30</p> <p>Время вводите в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС</p> <p>Между датой и временем должен быть только один пробел. Пробелов перед датой и после времени быть не должно.</p>

по умолчанию там стоит:

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*</Select>
  </Query>
</QueryList>
```

№5:

0) для подключения: `ssh user@frail.ibst.psu`

1) скопировать то, что напечатает в терминал сразу после подключения

2) создать группу: `sudo groupadd GNAME`

создать пользователя: `sudo useradd -m UNAME`

добавить пользователя в группу: `sudo usermod GNAME -aG UNAME`

удалить пользователя из группы: `sudo gpasswd -d UNAME GNAME`

3) назначить права ACL:

```
sudo setfacl -m u:UNAME:RULES, ..., DFNAME
```

```
sudo setfacl -m g:GNAME:RULES, ..., DFNAME
```

(ПРИМЕР:

```
sudo groupadd managers
```

```
sudo groupadd programmers
```

```
sudo useradd -m borisov
```

```
sudo useradd -m mihaylov
```

```
sudo useradd -m volodin
```

```
sudo useradd -m mironov
```

```
sudo usermod managers -aG borisov
```

```
sudo usermod managers -aG mihaylov
```

```
sudo usermod programmers -aG borisov
```

```
sudo usermod programmers -aG volodin
```

```
sudo setfacl -m g:managers:r-- employees
```

```
sudo setfacl -m g:programmers:r-- employees
```

```
sudo setfacl -m o::--- employees
```

```
sudo setfacl -m g:managers:rw- projects
```

```
sudo setfacl -m g:programmers:--- projects
```

```
sudo setfacl -m o::--- projects
```

```
sudo setfacl -m g:managers:rw- contracts
sudo setfacl -m g:programmers:rw- contracts
sudo setfacl -m o:--- contracts
```

4) команда `result` и копируем ее вывод

Вопрос 5
Выполнен
Балл: 5,00
Отметить вопрос

Подключитесь, используя протокол **ssh**, к Linux-системе по адресу **frail.libst.psu** как пользователь **user** с паролем **user123** (при подключении возможна задержка от нескольких секунд до нескольких минут).

1. Скопируйте задание в поле ответа теста.
2. Затем создайте указанные в задании учетные записи групп и пользователей.
3. После этого назначьте права доступа на папки и вложенные файлы, как указано в матрице доступа.
4. По окончании выполнения задания выполните команду **result** и скопируйте результат ее выполнения в поле ответа теста.

Время работы в системе ограничено 30 минутами.

Задание:
VARIANT 01.22.06.08.48

Users and Groups:

USER/GRP	managers	programmers
borisov	+	+
mihaylov	+	-
volodin	-	+
mironov	-	-

Access Matrix:

DIR/GRP	managers	programmers	OTHER
employees	R	R	-
projects	RW	-	-
contracts	RW	RW	-

```
Order:Variant: 01.22.06.08.48
managers: borisov mihaylov
programmers: borisov volodin
getfacl: Removing leading '/' from absolute path names
# file: documents/contracts
USER root      rw-
GROUP root     r-x
group managers rw-
group programmers rw-
mask programmers rw-
other          ---

# file: documents/employees
USER root      rw-
GROUP root     r-x
group managers r--
group programmers r--
mask programmers r-x
other          ---

# file: documents/projects
USER root      rw-
GROUP root     r-x
group managers rw-
mask programmers rw-
other          ---
```

Вопрос **Инфо**

🚩 Отметить вопрос

1. Запустите виртуальную машину Deb12-Exam
2. Подключитесь к виртуальной машине по протоколу **SSH**, используя адрес **localhost** и порт **2022**.
3. Для аутентификации используйте учетную запись **ibst** с паролем **lbst123**

№6:

0) подключиться к BM: `ssh -p 2022 ibst@localhost`

1) найти процесс, использующий порт **N**:

```
ss -tulnp | grep :[N]
```

2) скопировать вывод этой команды

3) найти сервис, запускающий этот процесс: `ps -o unit PID`

ИЛИ `systemctl status PID`

4) скопировать вывод этой команды

Вопрос **6**

Выполнен

Баллов: 4,00 из 4,00

🚩 Отметить вопрос

Задание

1. Найдите процесс, использующий порт 68
2. Найдите сервис, запускающий данный процесс

В поле ответа:

1. запишите команду для поиска процесса, использующего порт 68
2. запишите результат работы (вывод) этой команды
3. запишите команду/команды, которые использовали для поиска сервиса
4. запишите результат работы (вывод) этой команды/команд

```
1. sudo ss -tulnp | grep :[68]
2. udp UNCONN 0 0 0.0.0.0:68
0.0.0.0:* users:(("dhclient",pid=533,fd=7))
3. ps -o unit 533
4. UNIT
ifup@enp0s3.service
```

№7:

1) найти источник сообщений (сервис):

```
sudo systemctl list-units | grep -i news
```

2) команда остановки сообщений (сервиса):

```
sudo systemctl stop kingdom_news.service
```

2.2) запрет автозапуска:

```
sudo systemctl disable kingdom_news.service
```

3) поток выдачи сообщений реализовывался с помощью процесса **kingdom_news.service**

3.1) вывести фрагмент журнала:

```
journalctl -t kingdom_news.service
```

Вопрос **7**

Выполнен

Баллов: 4,00 из 4,00

🚩 Отметить вопрос

Задание

1. Остановите поток "Местных новостей"
2. Проверьте, что после перезагрузки сообщений нет

В поле ответа:

1. запишите команду/команды поиска источника сообщений
2. запишите команду/команды остановки выдачи сообщений
3. объясните, как стартовал и работал поток выдачи сообщений

1. `sudo systemctl list-units | grep -i news`
2. `sudo systemctl stop kingdom_news.service`
`sudo systemctl disable kingdom_news.service`
3. янв 01 19:24:34 exam2025 systemd[1]:

№8:

1) найти все активные процессы: (возможно процесс **oracul.service**)

```
sudo ps -a
```

1.2) информация о нужном процессе:

```
ps -o unit PID
```

2) остановка процесса:

```
sudo systemctl stop user@1002.service
```

2.2) запрет автозапуска:

```
sudo systemctl disable user@1002.service
```

3) поток выдачи сообщений реализовывался с помощью процесса [user@1002.service](#)

3.1) вывести фрагмент журнала:

```
journalctl -t user@1002.service
```

Вопрос **8**

Выполнен

Баллов: 4,00 из 4,00

🚩 Отметить вопрос

Задание

1. Остановите поток предсказаний "Оракула"
2. Проверьте, что после перезагрузки сообщений нет

В поле ответа:

1. запишите команду/команды поиска источника сообщений
2. запишите команду/команды остановки выдачи сообщений
3. объясните, как стартовал и работал поток выдачи сообщений

Hint:

```
export XDG_RUNTIME_DIR="/run/user/$UID"
export DBUS_SESSION_BUS_ADDRESS="unix:
```

1. ps -aux - посмотрел процессы
ps -o unit 634 - получил информацию о unit, который связан с PID=634
2. sudo systemctl stop user@1002.service
3. Поток выдачи сообщений оракула реализовывался с помощью процесса
systemctl status user@1002.service
● user@1002.service - User Manager for UID 1002

№9:

1) найти все активные процессы:

```
sudo ps -a
```

1.2) информация о нужном процессе:

```
ps -o unit PID
```

2) остановка процесса:

```
sudo systemctl stop SNAME.service
```

2.2) запрет автозапуска:

```
sudo systemctl disable SNAME.service
```

3) поток выдачи сообщений реализовывался с помощью процесса **SNAME.service**

3.1) вывести фрагмент журнала:

```
journalctl -t SNAME.service
```

Вопрос 

Нет ответа

Балл: 4,00

 Отметить вопрос

Задание

1. Остановите поток сообщений из "Странного места"
2. Проверьте, что после перезагрузки сообщений нет

В поле ответа:

1. запишите команду/команды поиска источника сообщений
2. запишите команду/команды остановки выдачи сообщений
3. объясните, как стартовал и работал поток выдачи сообщений

(возможно: strange place, weird odd, curious unusual, area)

странный прил

- 1 **strange** **curious** **singular** **unusual** **extraordinary**
необычный, любопытный, особый
- 2 **odd** **weird** **queer** **peculiar** **freak**
необычный, непонятный, своеобразный
- 3 **bizarre** **quaint** **freaky** **freakish**
причудливый

место сущ средний род

- 1 **place** **spot** **position** **point** **location** **situation**
местечко, точка, положение, расположение
- 2 **site** **station**
участок
- 3 **space** **room**
пространство, номер

№10

1) найти все процессы:

```
sudo ps -a
```

1.2) информация о нужном процессе:

```
ps -o unit PID
```

2) остановка процесса:

```
sudo systemctl stop SNAME.service
```

2.2) запрет автозапуска:

```
sudo systemctl disable SNAME.service
```

3) поток выдачи сообщений реализовывался с помощью процесса **SNAME**.service

3.1) вывести фрагмент журнала:

```
journalctl -t kingdom_news.service
```

Вопрос **10**

Нет ответа

Балл: 4,00

🚩 Отметить вопрос

Задание

1. Остановите поток сообщений "Слава богу, ты пришел ..."
2. Проверьте, что после перезагрузки сообщений нет

В поле ответа:

1. запишите команду/команды поиска источника сообщений
2. запишите команду/команды остановки выдачи сообщений
3. объясните, как стартовал и работал поток выдачи сообщений

(возможно процесс называется *thank god you came*)

№11: все попытки аутентификации с использованием команды **COMMAND** пользователем **UNAME**

для удачных: дата и время захода и выхода писать вручную

для неудачных: дата время попытки и причина отказа писать вручную

`sudo journalctl -t COMMAND | grep UNAME`

ВХОД И ВЫХОД - ГДЕ ОДИНАКОВЫЙ
`login [N]`

дата
время

```
user@ibst-lab-5:~$ sudo journalctl -t login | grep test2
янв 25 17:53:16 ibst-lab-5 login[650]: pam_unix(login:session): session opened for user test2(uid=1004) by LOGIN(uid=0)
янв 25 17:54:42 ibst-lab-5 login[619]: pam_unix(login:session): session opened for user test2(uid=1004) by LOGIN(uid=0)
янв 25 17:54:43 ibst-lab-5 login[619]: pam_unix(login:session): session closed for user test2
янв 25 17:54:49 ibst-lab-5 login[638]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=test2
янв 25 17:54:52 ibst-lab-5 login[638]: FAILED LOGIN (1) on '/dev/tty1' FOR 'test2', Authentication failure
user@ibst-lab-5:~$ _
```

причина отказа ?

Вопрос 11

Выполнен

Баллов: 2,00 из 3,00

Отметить вопрос

Найдите все попытки аутентификации с использованием команды **login** пользователем **robber**

Ответы для удачных попыток запишите в формате

Дата Время входа, Дата Время выхода

Для неудачных в формате

Дата Время попытки, причину отказа

Дату записать в формате ГГГГ-ММ-ДД

Время записать в формате ЧЧ:ММ:СС

Например:

2026-01-01 13:25:01, 2026-01-01 14:12:45

2026-01-07 19:20:21, ошибка аутентификации

```
ibst@exam2025:/etc/systemd/system$ sudo journalctl _COMM=login | grep robber
дек 25 21:32:19 exam2025 login[2145]: pam_unix(login:session): session opened for user robber(uid=1014) by root(uid=0)
дек 25 21:32:24 exam2025 login[2145]: pam_unix(login:session): session closed for user robber
дек 26 07:57:19 exam2025 login[625]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=robber
дек 26 07:57:22 exam2025 login[625]: FAILED LOGIN (1) on '/dev/tty1' FOR 'robber', Authentication failure
дек 26 07:57:58 exam2025 login[625]: FAILED LOGIN (2) on '/dev/tty1' FOR 'robber', Authentication failure
дек 26 22:02:46 exam2025 login[566]: FAILED LOGIN (1) on '/dev/tty1' FOR 'robber', Permission denied
```

№12:

`sudo journalctl -u ssh | grep queen`

Вопрос 12

Выполнен

Баллов: 2,80 из 3,00

Отметить вопрос

Найдите все попытки удаленной аутентификации через службу **ssh** пользователем **queen**

Ответы для удачных попыток запишите в формате

Дата Входа, Дата Выхода, IP адрес

В качестве времени входа и выхода использовать время начала и конца сессии.

Для неудачных в формате

Дата Входа, Выхода, причину отказа, IP адрес

В качестве времени попытки использовать время проверки пароля.

Дату записать в формате ГГГГ-ММ-ДД

Время записать в формате ЧЧ:ММ:СС

Например:

2026-01-01 13:25:01, 2026-01-01 14:12:45, 192.168.3.123

2025-12-28 11:26:54 неправильный пароль 10.0.2.2 port 43706

2025-12-28 11:27:00 неправильный пароль 10.0.2.2 port 43706

2025-12-28 11:27:05 неправильный пароль 10.0.2.2 port 43706

2025-12-28 11:27:06 неправильный пароль 10.0.2.2 port 43706

2025-12-28 11:38:25 2025-12-28 11:39:34 10.0.2.2 port 47532

2025-12-28 14:58:03 2025-12-28 14:58:54 10.0.2.2 port 53932

дата время входа

дата время выхода

причина отказа

??

IP адрес

```
user@ibst-lab-5:~$ sudo journalctl -u ssh | grep user
ноя 16 22:33:20 ibst-lab-5 sshd[616]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2 user=root
ноя 16 22:33:48 ibst-lab-5 sshd[616]: Connection reset by authenticating user root 10.0.2.2 port 57253 [preauth]
ноя 16 22:33:48 ibst-lab-5 sshd[616]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2 user=root
ноя 16 22:34:25 ibst-lab-5 sshd[620]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2 user=root
ноя 16 22:35:02 ibst-lab-5 sshd[620]: Connection reset by authenticating user root 10.0.2.2 port 57257 [preauth]
ноя 16 22:35:15 ibst-lab-5 sshd[622]: Accepted password for user from 10.0.2.2 port 57319 ssh2
ноя 16 22:35:15 ibst-lab-5 sshd[622]: pam_unix(sshd:session): session opened for user user(uid=1000) by (uid=0)
ноя 16 22:35:15 ibst-lab-5 sshd[622]: pam_env(sshd:session): deprecated reading of user environment enabled
ноя 16 22:35:15 ibst-lab-5 sshd[622]: pam_unix(sshd:session): session closed for user user
ноя 16 22:39:59 ibst-lab-5 sshd[642]: Accepted password for user from 10.0.2.2 port 57496 ssh2
ноя 16 22:39:59 ibst-lab-5 sshd[642]: pam_unix(sshd:session): session opened for user user(uid=1000) by (uid=0)
ноя 16 22:39:59 ibst-lab-5 sshd[642]: pam_env(sshd:session): deprecated reading of user environment enabled
ноя 16 22:39:59 ibst-lab-5 sshd[642]: pam_unix(sshd:session): session closed for user user
ноя 16 22:40:26 ibst-lab-5 sshd[663]: Accepted publickey for user from 10.0.2.2 port 57504 ssh2: RSA SHA256:fCYuGQVRSJuGVCScR0cy6xFDL1RTJnRNaSGEurv41ZQ
ноя 16 22:40:26 ibst-lab-5 sshd[663]: pam_unix(sshd:session): session opened for user user(uid=1000) by (uid=0)
ноя 16 22:40:26 ibst-lab-5 sshd[663]: pam_env(sshd:session): deprecated reading of user environment enabled
user@ibst-lab-5:~$ _
```

№13: все попытки использования команды **COMMAND** пользователем **UNAME**

`sudo journalctl -t COMMAND | grep UNAME`

дата, время, результат, от чьего имени, команда

для команды sudo всегда будет от имени root

дата время от чьего имени команда

```
январь 25 17:59:23 ibst-lab-5 sudo[680]: user : TTY=ttty1 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/cat /home/user/.bash_history
январь 25 17:59:23 ibst-lab-5 sudo[680]: pam_unix(sudo:session): session opened for user root(uid=0) by user(uid=1000)
январь 25 17:59:23 ibst-lab-5 sudo[680]: pam_unix(sudo:session): session closed for user root
январь 25 18:00:25 ibst-lab-5 sudo[684]: user : TTY=ttty1 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/journalctl -t sudo
январь 25 18:00:25 ibst-lab-5 sudo[684]: pam_unix(sudo:session): session opened for user root(uid=0) by user(uid=1000)
user@ibst-lab-5:~$ _
```

результат или "успех" или

```
январь 25 18:07:24 ibst-lab-5 sudo[703]: pam_unix(sudo:auth): authentication failure; logname=user uid=1000 euid=0 tty=/dev/tty1 ruser=user rhost= user=user
январь 25 18:07:36 ibst-lab-5 sudo[703]: user : 3 incorrect password attempts ; TTY=ttty1 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/ls
январь 25 18:07:44 ibst-lab-5 sudo[704]: user : TTY=ttty1 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/journalctl -t sudo
январь 25 18:07:44 ibst-lab-5 sudo[704]: pam_unix(sudo:session): session opened for user root(uid=0) by user(uid=1000)
user@ibst-lab-5:~$ _
```

Вопрос **13**

Выполнен

Баллов: 3,00 из 3,00

Отметить вопрос

Найдите все попытки использования команды **sudo** пользователем **prince**

Ответы запишите в формате

Дата, Время, Результат, От чьего имени, Команда

Дату записать в формате ГГГГ-ММ-ДД

Время записать в формате ЧЧ:ММ:СС

Результат записать как "Успех" при успешном выполнении команды, либо указать причину отказа при неуспешном.

Например:

2026-01-01, 13:06:25, "Команда не разрешена", root, /usr/bin/cat /etc/shadow

2025-12-26, 22:47:15, успех, root, /usr/bin/ls /home/queen

2025-12-26, 22:47:21, успех, root, /usr/bin/ls /home/queen

2025-12-26, 22:47:29, успех, root, /usr/bin/ls /home/queen -l

2025-12-26, 22:47:59, успех, root, /usr/bin/ls /home/ibst

2025-12-26, 22:48:03, успех, root, /usr/bin/ls /home/ibst -la

2025-12-26, 22:48:12, успех, root, /usr/bin/ls /home/quin -la

2025-12-26, 22:48:18, успех, root, /usr/bin/ls /home/queen -la

2025-12-26, 22:49:23, command not allowed, root, /usr/bin/ls /root -la

2025-12-28, 14:57:14, успех, root, /usr/local/bin/drink_with_friends