ЧАСТЬ ВИНДОВС----------

ВОПРОС 1 (1б)

Указать пользователей в алфавитном порядке. (Отключенные учетки вроде как не надо)

Как сделать:

1) WIN+R → lusrmgr.msc →Пользователи. Потом отсортировать.

ВОПРОС 2 (1б)

Указать пользователей, входящих в группу.

Как сделать:

То же самое, что и в первом задании, открываем папку «Группы» и тыкаем на нужную
группу. Там вылезает список пользователей.

ВОПРОС 3-4 (по 2б)

Для пользователя … определите:

А) Время последнего удачного входа в систему

Б) Время последней неудачной аутентификации

Как сделать:

В поиске пишем «Просмотр событий» → Журналы Windows → Безопасность.

В правой панели при помощи фильтра выбираем соответствующего пользователя и коды
событий:

4624 — удачная аутентификация

4625 — неудачная аутентификация

Не косячим с форматом даты и времени !

ЧАСТЬ ЛИНУКС----------

ВОПРОС 5 (5б)

Подключитесь, используя протокол ssh, к Linux-системе по адресу frail.ibst.psu как
пользователь user с паролем user123.

Как сделать:

Осуществляем соединение с помощью команды ssh user@frail.ibst.psu

Далее создаем группы с помощью sudo groupadd

Создаем пользователей, если нет, с помощью sudo useradd -m -g «группа» «имя
пользователя»

Добавляем пользователей в группы с помощью команд sudo usermod -aG «группа» «имя
пользователя»

Дана некая матрица прав доступа с буквами, по ней выдаем права.

ls – просмотреть содержимое каталога

cd – перейти в папку

setfacl -m u:alice:rwx «путь» — выдать ВСЕ права пользователю alice.
setfacl -m g:developers:r-x «путь» – выдать права на чтение и выполнение группе developers
setfacl -x u:alice «путь» - удалить права в случае косяка
Пишем result, копируем результат в ответ. Эту команду можно писать много раз, чтобы
сверяться с матрицей.

ВОПРОС 6. (4б)
Найдите процесс, использующий порт 68. Найдите сервис, запускающий этот процесс.
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 — наш идентификатор !!!
4 UNIT ifup@enp0s3.service

Вопрос 7 (4б)
Остановите поток новостей. Проверьте, что после перезагрузки сообщений нет.
1. ps -aux – просмотр, запущен ли этот процесс с новостями. Также тут покажет путь к файлу
сервиса !
ls -a /etc/systemd/system – для просмотра конфигурационного файла сервиса
2. sudo systemctl stop penzainform.service – остановить процесс
sudo systemctl disable penzainform.service – убрать автозагрузку
sudo systemctl status penzainform.service – смотрим, все ли мы сделали правильно
3. Сервис находился в автозагрузке и запускался с каждым пуском системы. Скрипт выдавал сообщения прямо в консоль

Вопрос 8 (4б)
Остановите поток предсказаний Оракула. Проверьте, что после перезагрузки сообщений нет
1. ps -aux – смотрим процесс и его PID.
ps -o unit PID – смотрим unit, который управляет этим процессом
2. sudo systemctl stop user@1002.service
sudo systemctl disable user@1002.service
sudo systemctl status user@1002.service
3. Сервис стартовал автоматически при загрузке системы через шаблонный сервис
user@1002.service, который запускал все процессы пользователя с UID 1002. Скрипт выводил
сообщения в консоль

Вопрос 9-10 . (по 4б)

Остановите поток сообщений из Странного места. Проверьте, что после перезагрузки
сообщений нет.
Остановите поток сообщений Слава богу, ты пришел …

1. systemctl list-unit-files --state=enabled Служба будет запускаться автоматически при старте системы или при достижении нужного target
2. systemctl list-units --type=service --state=running Показывает службы, которые сейчас запущены и работают

Вопрос 11. (3б)
robber.
Найдите все попытки аутентификации с использованием команды login пользователем
sudo journalctl _COMM=login -o short-iso | grep robber | grep -E "(session opened|session closed)"
Данная команда группирует события открытия и закрытия одной сессии (там видно идентификатор).
sudo journalctl _COMM=login -o short-iso | grep robber | grep "authentication failure"
Неудачные попытки входа
Вручную преобразовать данные и записать ответ в нужном формате.

Вопрос 12. (3б)
Найдите все попытки удаленной аутентификации через службу SSH пользователем queen
sudo journalctl _COMM=sshd -o short-iso | grep queen | grep -E “opened|closed”
или
sudo journalctl _COMM=sshd-session -o short-iso | grep sanek | grep -E "opened|closed" – для просмотра сессий, а именно даты их открытия и закрытия. Смотрим по PID.
КЛЮЧЕВЫЕ СЛОВА В ЖУРНАЛЕ:
session opened
session closed
sudo journalctl _COMM=sshd -o short-iso | grep queen | grep -E “Failed”
или
sudo journalctl _COMM=sshd-session -o short-iso | grep sanek | grep -E "Failed" – ввод неудачного пароля
КЛЮЧЕВЫЕ СЛОВА В ЖУРНАЛЕ:
Failed password

Вопрос 13. (3б)
Найдите все попытки использования команды sudo пользователем prince
sudo journalctl _COMM=sudo -o short-iso | grep "prince"

Ответы:
Текст вопроса

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

2025-12-25 21:32:19 начало сеанса
2025-12-25 21:32:24сеанс завершен
2026-12-26 07:57:19 ошибка аутентификации
2026-12-26 07:57:22 ошибка аутентификации
2026-12-26 07:57:58 ошибка аутентификации
2026-12-26 22:02:46 отклонено

____ Windows_____
Запустите виртуальную машину Exam-2022.
Используйте логин ИБСТ и пароль Ибст123 для входа в систему.
Ответьте на вопросы последующих тестов.
1)Перечислите найденных пользователей в порядке алфавита. Отключенные учетные записи не учитывать. Учетную запись, под которой авторизовались в системе тоже не учитывать.
Ответ:
Drobyna,Ivanov,Lemzyaikin,Levsky,Mochkasov,Nevsky,Ogulo,
Petrov,Shemysheikin,Sheptalo,Sidorov
2)
1.Отметьте пользователей, входящих в группу "Администраторы"
Ответ:Ogulo,ИБСТ,Nevsky
2.Отметьте пользователей, входящих в группу "Криптографические операторы"
Ответ:Sheptalo,Drobyna
3.Отметьте пользователей, входящих в группу "Операторы настройки сети"
Ответ:Ivanov,Sidorov
4.Отметьте пользователей, входящих в группу "Операторы архива"
Ответ:Levsky,Petrov
3)
1.Для пользователя Shemysheikin определите:
время последнего удачного входа в систему:16.05.2017 08:56:55
время последней неудачной аутентификации: 30.12.2021 12:38:46
2.Для пользователя Drobyna определите:
время последнего удачного входа в систему:12.05.2017 16:28:08
время последней неудачной аутентификации:30.12.2021 12:36:46
3.Для пользователя Nevsky определите:
время последнего удачного входа в систему:
время последней неудачной аутентификации:30.12.2021 12:38:12
4.Для пользователя Ivanov определите:
время последнего удачного входа в систему:12.05.2017 16:29:51
время последней неудачной аутентификации:30.12.2021 12:37:13
5.Для пользователя Lemzyaikin определите:
время последнего удачного входа в систему:12.05.2017 16:43:52
время последней неудачной аутентификации:30.12.2021 12:37:40
6.Для пользователя Levsky определите:
время последнего удачного входа в систему:12.05.2017 16:43:07
время последней неудачной аутентификации:30.12.2021 12:45:20
7.Для пользователя Mochkasov определите:
время последнего удачного входа в систему:12.05.2017 16:44:28
время последней неудачной аутентификации:12.05.2017 16:30:28
8.Для пользователя Sheptalo определите:

время последнего удачного входа в систему:12.05.2017 16:40:42
время последней неудачной аутентификации:16.05.2017 08:54:57