Кейс 1: Установка и настройка SSH-сервера

Задание:

1. Установить SSH-сервер на виртуальную машину (например, с помощью `sudo apt-get install openssh-server`).
2. Настроить SSH-сервер, убедиться, что он запущен, и проверить его статус.

Ожидаемый результат:

- SSH-сервер установлен и запущен.
- Статус SSH-сервера проверен и отображается как "running".

Кейс 2: Подключение к удаленному серверу

Задание:

1. Использовать команду `ssh` для подключения к удаленному серверу.
2. Подключиться к серверу с использованием имени пользователя и IP-адреса (например, `ssh user@192.168.1.100`).

Ожидаемый результат:

- Успешное подключение к удаленному серверу через SSH.

Кейс 3: Копирование файлов с помощью SCP

Задание:

1. Использовать команду `scp` для копирования файла с локальной машины на удаленный сервер.
2. Копировать файл с удаленного сервера на локальную машину.

Ожидаемый результат:

- Файл успешно скопирован на удаленный сервер и обратно на локальную машину.

Кейс 4: Работа с ключами SSH

Задание:

1. Сгенерировать пару ключей SSH с помощью команды `ssh-keygen`.
2. Добавить публичный ключ на удаленный сервер для безпарольного входа.
3. Подключиться к серверу с использованием ключей SSH.

Ожидаемый результат:

- Пара ключей SSH сгенерирована.
- Публичный ключ добавлен на удаленный сервер.
- Успешное подключение к серверу без ввода пароля.

Кейс 5: Настройка файла конфигурации SSH

Задание:

1. Создать или отредактировать файл конфигурации SSH (`~/.ssh/config`).
2. Добавить алиас для быстрого подключения к серверу (например, задать имя сервера и ключи).

Ожидаемый результат:

- Файл конфигурации SSH настроен.
- Успешное подключение к серверу с использованием алиаса.

Кейс 6: Перенаправление портов (Port Forwarding)

Задание:

1. Настроить локальное перенаправление порта (например, перенаправить локальный порт 8080 на удаленный порт 80).
2. Проверить доступность удаленного сервера через локальный порт.

Ожидаемый результат:

- Локальное перенаправление порта настроено.
- Удаленный сервер доступен через локальный порт.

Кейс 7: Управление сеансами SSH с помощью tmux/screen

Задание:

1. Установить и настроить `tmux` или `screen` на удаленном сервере.
2. Создать и управлять сеансами для долгосрочных задач, проверяя их статус после отключения и повторного подключения.

Ожидаемый результат:

- `tmux` или `screen` установлен и настроен.
- Созданы и управляются сеансы SSH для выполнения долгосрочных задач.

Кейс 8: Безопасность SSH

Задание:

1. Ограничить доступ к SSH путем изменения порта по умолчанию.
2. Запретить вход по паролю, разрешив только вход по ключам.

3. Ограничить доступ по IP-адресам.

Ожидаемый результат:

- Порт по умолчанию для SSH изменен.
- Вход по паролю запрещен, вход по ключам разрешен.
- Доступ к SSH ограничен по IP-адресам.

Кейс 9: Установка и использование SSH-агента

Задание:

1. Настроить и запустить SSH-агент на локальной машине.
2. Добавить ключи в SSH-агент и использовать их для подключения к удаленным серверам.

Ожидаемый результат:

- SSH-агент настроен и запущен.
- Ключи добавлены в SSH-агент и успешно используются для подключения.

Кейс 10: Создание и использование бастион-сервера

Задание:

1. Настроить бастион-сервер для доступа к другим серверам внутри защищенной сети.
2. Подключаться к внутренним серверам через бастион-сервер.

Ожидаемый результат:

- Бастион-сервер настроен.
- Успешное подключение к внутренним серверам через бастион-сервер.