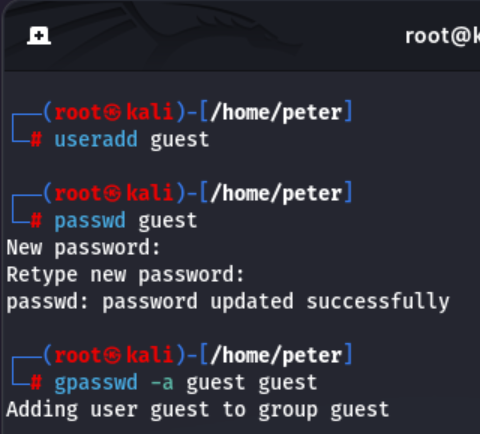
**Практическая работа 7**

Создайте учётную запись пользователя guest

Установите пароль пользователю

Также добавьте пользователя guest в группу guest:



Создайте домашнюю директорию пользователю guest

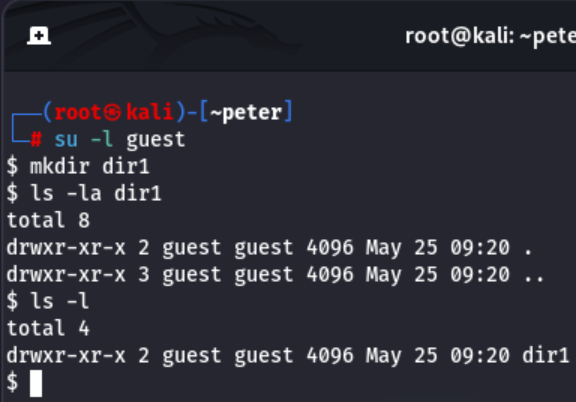
Смените владельца данной директории на guest и отредактируйте файл /etc/passwd:



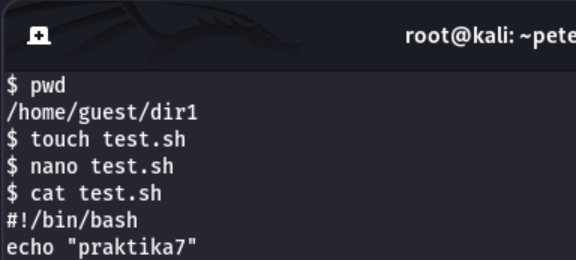
Смените пользователя на guest

Создайте директорию в домашней папке пользователя guest

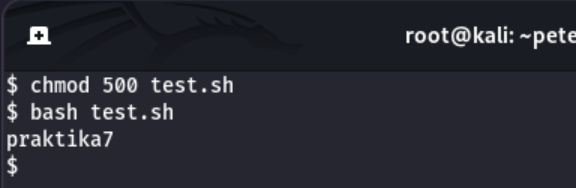
Посмотрите список файлов в директории и права доступа к ним:



Создадим исполняемый файл следующего вида и попробуем выполнить этот файл:



Для выполнения файла ему необходимо установить права:



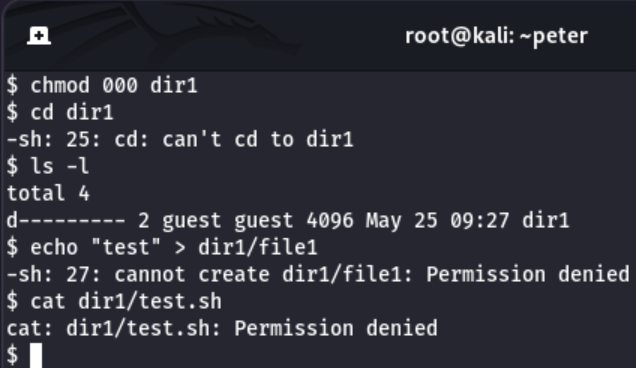
Удалим все права на директорию dir1

Попробуем просмотреть содержимое директории

Попробуем создать файл file1

Попробуем прочитать файл test.sh

Какой результат всех этих действий? ***(отказ в доступе):***



Установим права 700 на директорию dir1

Попробуем просмотреть содержимое директории

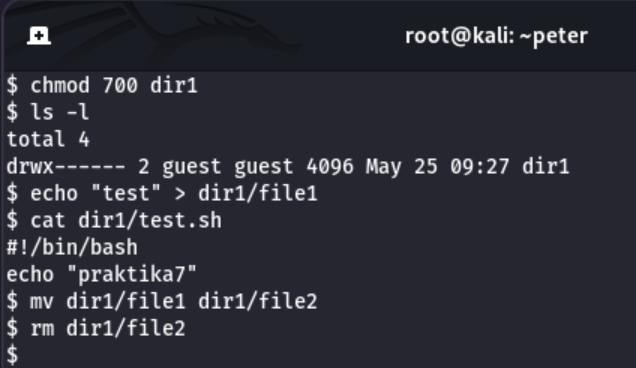
Попробуем создать файл file1

Попробуем прочитать файл test.sh

Попробуем переименовать файл file1 в file2

Попробуем удалить file2

Какой результат всех этих действий? ***(успешное выполнение):***



|  |  |  |
| --- | --- | --- |
| Директория | Разрешение | Действия |
| d--------- | 000 | - |
| d--x------ | 100 | Исполнение(владельцем) |
| d-w------- | 200 | изменение(владельцем) |
| drwx------ | 700 | Любые действия(владельцем) |
| drwxr-x--- | 750 | Любые действия(владельцем), чтение и исполнение(группой) |
| drwxrw-r-- | 754 | Любые действия(владельцем), чтение и изменение(группой), чтение другими пользователями |
| drwxrwxr-x | 775 | Любые действия(владельцем), любые действия группой(группой), чтение и исполнение другими пользователями |

\*Изменение – создание/удаление/переименовывание/запись

|  |  |  |
| --- | --- | --- |
| Операция | Минимальные права на директорию(421; rwx) | Минимальные права на файл (поддиректорию) |
| Создание файла | 020(-w-) | - |
| Удаление файла | 020(-w-) | - |
| Чтение файла | 400(r--) | r |
| Запись в файл | 020(-w-) | w |
| Переименование файла | 020(-w-) | w |
| Создание поддиректории | 020(-w-) | - |
| Удаление поддиректории | 020(-w-) | - |

**Ответы на вопросы**

**1. Конфигурация подсистемы защиты в ОС:**

Подсистема защиты в операционных системах (ОС) отвечает за управление доступом к ресурсам системы, предотвращение несанкционированного доступа и обеспечение безопасности данных. Конфигурация этой подсистемы включает настройку политики безопасности, создание и управление учетными записями пользователей, настройку прав доступа к файлам и приложениям, а также настройку механизмов журналирования и аудита событий безопасности.

**2. Механизм идентификации пользователей в ОС:**

Идентификация пользователей заключается в распознавании пользователя по уникальному идентификатору, такому как логин или идентификационный номер. Это первый шаг в процессе контроля доступа, который позволяет ОС определить, кто пытается получить доступ к системе.

**3. Механизм аутентификации пользователей в ОС:**

Аутентификация подтверждает подлинность пользователя, который пытается получить доступ к системе, проверяя предоставленные им учетные данные, такие как пароль, смарт-карта, отпечаток пальца и другие биометрические данные. Популярные методы включают пароли, одноразовые коды, биометрическую аутентификацию и двухфакторную аутентификацию (2FA).

**4. Основные механизмы защиты в ОС:**

Основные механизмы защиты включают контроль доступа, шифрование данных, механизмы аудита и журналирования, антивирусное и антишпионское программное обеспечение, а также применение патчей и обновлений для устранения уязвимостей.

**5. Классификация угроз:**

Угрозы безопасности можно классифицировать на внешние (например, хакеры, вредоносное ПО) и внутренние (недобросовестные сотрудники). Также они делятся на пассивные (перехват данных) и активные (модификация данных).

**6. Авторизация. Разграничение доступа к объектам ОС:**

Авторизация определяет права и привилегии пользователя после его аутентификации. Разграничение доступа включает в себя установление и применение правил доступа к ресурсам ОС, таких как файлы, приложения и сетевые ресурсы, на основе ролей и разрешений.

**7. Аудит системы защиты:**

Аудит системы защиты включает мониторинг и запись действий пользователей и событий системы для анализа и обнаружения попыток несанкционированного доступа, нарушения политики безопасности или других подозрительных действий.

**8. Системы защиты программного обеспечения:**

Системы защиты ПО включают антивирусные программы, фаерволы, системы обнаружения и предотвращения вторжений (IDS/IPS), средства шифрования и инструменты управления патчами.

**9. Атаки на операционные системы:**

Атаки на ОС могут включать вирусы, черви, трояны, эксплойты, атаки на отказ в обслуживании (DoS), атаки с целью повышения привилегий и атакующие, использующие уязвимости в программном обеспечении.

**10. Защищенные операционные системы:**

Защищенные ОС разработаны с усиленными мерами безопасности и включают функции, такие как мандатный контроль доступа, многоуровневую защиту данных и изоляцию процессов. Примеры включают SELinux и Windows с включенной BitLocker.

**11. Получение данных авторизации и другой ключевой информации:**

Способы получения данных авторизации могут включать фишинг, атаки грубой силы, перехват данных (sniffing), а также использование вредоносных программ для кражи паролей.

**12. Восстановление удаленных данных (сборка мусора):**

Восстановление удаленных данных включает использование специальных программ для восстановления файлов, которые были удалены, но не перезаписаны на жестком диске. Сборка мусора — это процесс управления памятью, который очищает неиспользуемые данные.

**13. Поиск и сбор информации:**

Поиск и сбор информации включают мониторинг системных логов, анализ сетевого трафика, использование утилит для сканирования уязвимостей и изучение данных, полученных от систем обнаружения вторжений.

**14. Аппаратная и биометрическая аутентификация:**

Аппаратная аутентификация может включать использование смарт-карт, токенов или TPM-чипов. Биометрическая аутентификация использует уникальные физические характеристики пользователя, такие как отпечатки пальцев, сетчатка глаза, голос или лицо.

**15. Модели управления доступом:**

Существуют различные модели управления доступом, такие как:

- Мандатное управление доступом (MAC): права доступа определяются центральным администратором и применяются независимо от желания пользователя.

- Дискреционное управление доступом (DAC): владелец ресурса определяет права доступа.

- Ролевое управление доступом (RBAC): права доступа определяются на основе ролей, назначаемых пользователям.

-Атрибутное управление доступом (ABAC): права доступа определяются на основе атрибутов пользователя, ресурса и контекста доступа.