МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение

высшего образования

**«Северный (Арктический) федеральный университет имени М.В. Ломоносова»**

|  |
| --- |
| Высшая школа информационных технологий и автоматизированных систем |

**ЛАБОРАТОРНАЯ РАБОТА №9**

|  |  |  |
| --- | --- | --- |
| По дисциплине: | | Защита информации в системах управления базами данных |
|  | | |
|  | | |
| На тему | Защита хоста | |
|  | | |
|  | | |

|  |  |
| --- | --- |
|  | Выполнил обучающийся:  Грозов Илья Владимирович |
|  |  |
|  | Направление подготовки / специальность:  10.03.01 Информационная безопасность |
|  |  |
|  | Курс: 3 |
|  | Группа: 151113 |
|  | Руководитель: Зубарев Александр Андреевич, ст. |
|  | преподаватель |
|  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Отметка о зачете |  |  |  |  |
|  |  |  |  |  |
| Руководитель |  |  |  | А.А. Зубарев. |
|  |  |  |  |  |

Архангельск 2024

##### Задание

Получить практический навык защиты хоста при эксплуатации СУБД

ХОД РАБОТЫ

**1 КОНФИГУРАЦИЯ КОНТЕЙНЕРА DOCKER С DEBAIN**

Конфигурация контейнера с debain невозможна в настоящий момент времени. Работа будет выполнена на обычной виртуальной машине Debian 11 с именем ZIvSYBD-LR9

**2 ECRYPTFS**

2.1 Установка eCryptfs

Выполним установку ecryptfs при помощи команды: sudo apt-get install ecryptfs-utils. Выполнение установки eCryptfs отображено на рисунке 1

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 – Выполнение установки eCryptfs

Завершение установки eCryptfs отображено на рисунке 2

Изображение выглядит как текст, снимок экрана, Шрифт, черно-белый

Автоматически созданное описание

Рисунок 2 – Завершение установки eCryptfs

2.2 Добавление пользователя cryptouser

Добавим пользователя cryptouser при помощи команды: sudo adduser cryptouser. Добавление пользователя cryptouser отображено на рисунке 3

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Рисунок 3 – Добавление пользователя cryptouser

Установим для пользователя cryptouser пароль и запрашиваемые данные. Установка пароля и запрашиваемых данных для пользователя cryptouser отображена на рисунке 4

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 4 – Установка пароля для пользователя cryptouser и запрашиваемых данных

Сменим пользователя на cryptouser для проверки корректности его создания. Смена пользователя отображена на рисунке 5

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок 5 – смена пользователя

Рабочий пользователь cryptouser отображен на рисунке 6

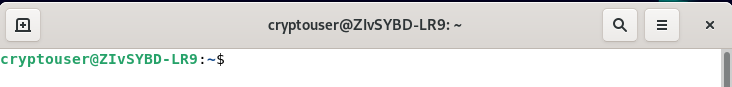


Рисунок 6 – Рабочий пользователь cryptouser

2.3 Шифрование домашнего каталога пользователя с помощью eCryptfs

Выполним шифрование домашней директории пользователя cryptouser. Перед выполнением шифрования нам необходимо дополнительно установить rsync. Установка rsync отображена на рисунке 7

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 7 – Установка rsync

Выполним шифрование домашнего каталога пользователя cryptouser при помощи команды sudo-ecryptfs-migrate-home -u cryptouser. Шифрование домашнего каталога пользователя cryptouser отображено на рисунке 8

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 8 – Шифрование домашнего каталога пользователя cryptouser

Шифрование было завершено неудачно. Было выяснено, что его невозможно произвести, поскольку системными процессами были открыты файлы, которые не позволяют завершить процесс шифрования. Создадим пользователя cryptouser2 для шифрования его домашнего каталога. Создание пользователя cryptouser2 отображено на рисунке 9

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок 9 – Создание пользователя cryptouser2

Выполним шифрование домашнего каталога пользователя cryptouser2 при помощи команды: sudo-ecryptfs-migrate-home -u cryptouser2. Выполнение шифрования отображено на рисунке 10

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 10 – Выполнение шифрования

Шифрование домашнего каталога пользователя cryptouser2 не было произведено из-за того, что не был загружен модуль. Загрузим модуль при помощи команды: sudo modprobe ecryptfs. Загрузка модуля отображена на рисунке 11



Рисунок 11 – Загрузка модуля

Модуль загружен. Выполним шифрование домашнего каталога пользователя cryptouser2 при помощи команды: sudo-ecryptfs-migrate-home -u cryptouser2. Выполнение шифрования отображено на рисунке 12

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 12 – Выполнение шифрования

Введем установленный пароль. После ввода пароля необходимо воспользоваться информацией выведенной в заметке. Заметка отображена на рисунке 13

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 13 – Заметка

Авторизуемся под пользователем cryptouser2. Авторизация под пользователем cryptouser2. Авторизация под пользователем cryptouser2 отображена на рисунке 14

Изображение выглядит как текст, снимок экрана, логотип, дизайн

Автоматически созданное описание

Рисунок 14 – Авторизация под пользователем cryptouser2

По информации в заметке удалим каталог cryptouser2.Gna5LAoP при помощи команды sudo rm -r cryptouser2.Gna5LAoP. Удаление каталога cryptouser2.Gna5LAoP отображено на рисунке 15

Изображение выглядит как текст, Шрифт, линия, программное обеспечение

Автоматически созданное описание

Рисунок 15 – Удаление каталога cryptouser2.Gna5LAoP

При помощи команды ecryptfs-unwrap-passphrase узнаем пароль для восстановления зашифрованного раздела. Получение пароля для восстановления отображено на рисунке 16

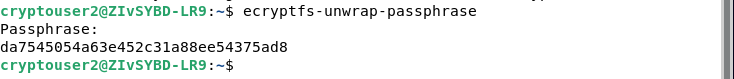


Рисунок 16 – Получение пароля для восстановления

**3 LUKS**

3.1 Установка поддержки luks

Установим luks при помощи команды: apt-get install cryptsetup. Установленный cryptsetup отображен на рисунке 17

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 17 – Установленный cryptsetup

3.2 Создание раздела

Для создания нового раздела под шифрование с luks воспользуемся инструментами virtualbox за место утилит Debian и создадим диск. В настройках виртуальной машины добавим новый диск. Добавление нового диска отображено на рисунке 18

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 18 – Добавление нового диска

Создадим новый диск с предложенным размером в 100 мегабайт. Создание диска отображено на рисунке 19

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 19 – Создание нового диска

Созданный новый диск отображен на рисунке 20

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 20 – Созданный новый диск

Подключим диск к виртуальной машине. Подключенный диск к виртуальной машине отображен на рисунке 21

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 21 – Подключенный диск к виртуальной машине

При помощи команды lsblk просмотрим, что диск виден системой. Просмотр диска отображен на рисунке 22

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Рисунок 22 – Просмотр диска

Новый диск был зарегистрирован в системе под именем sbd

3.3 Шифрование созданного раздела

Выполним шифрование при помощи команды: sudo cryptsetup luksFormat /dev/sdb. Подтвердим свои действия введя заглавными буквами YES. Введем пароль по требованию. Завершенное шифрование отображено на рисунке 23

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 23 – Завершенное шифрование

**4 APPARMOR**

4.1 Установка apparmor

Выполним установку при помощи apt-get install apparmor. Уставнока apparmor отображена на рисунке 24

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 24 – Установка apparmor

Установим дополнительный пакет утилит при помощи команды: apt-get install apparmor-utils. Установка дополнительного пакета отображена на рисунке 25

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

Рисунок 25 – Установка дополнительного пакета

При помощи команды: systemctl status apparmor проверим, что apparmor запущен в системе. Проверка запуска apparmor в системе отображена на рисунке 26

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 26 – Проверка запуска apparmor в системе

Дополнительно загрузим пакет с профилями при помощи команды apparmor-profiles. Загрузка пакета с профилями отображена на рисунке 27

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 27 – Загрузка пакета с профилями

Проверим статус работы apparmor при помощи команды: sudo apparmor\_status. Проверка статуса работы apparmor отображена на рисунке 28

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 28 – Проверка статуса работы apparmor

При необходимости выполним перемещение ранее загруженных необходимых профилей при помощи команды mv. Перемещение профилей отображено на рисунке 29

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 29 – Перемещение профилей

4.2 Выполнение блокирования и разблокирования приложения

При помощи команды sudo aa-genprof /usr/bin/firefox начнем запись для последующей блокировки приложения. Путь указывает на расположение бинарного файла блокируемого приложения. В качестве блокируемого приложения был выбран браузер firefox. Запись для блокировки приложения отображена на рисунке 30

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 30 – Запись для блокирования приложения

Войдем в браузер, проделаем хаотичные действия, введем запрос кто такие гугеноты. Хаотичные действия в браузере отображены на рисунке 31

Изображение выглядит как текст, программное обеспечение, веб-страница, Веб-сайт

Автоматически созданное описание

Рисунок 31 – Хаотичные действия в браузере

Для простора событий можно использовать клавишу S, Просмотр событий отображен на рисунке 32

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 32 – Просмотр событий

Остановить запись для блокирования приложения можно по клавише F. Остановка записи отображена на рисунке 33

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 33 – Остановка записи событий

Теперь приложение должно быть заблокировано. Попробуем запустить приложение из терминала. Попытка запуска приложения отображена на рисунке 43



Рисунок 34 – Попытка запуска приложения

Приложение заблокировано

4.3 Удаление apparmor

Перед удалением apparmor необходимо остановить его системный процесс при помощи команды: /etc/init.d/apparmor stop. Отсановка системного процесса apparmor отображена на рисунке 35



Рисунок 35 – Остановка системного процесса apparmor

Выполним удаление apparmor и его зависимостей при помощи команды: sudo apt-get remove apparmor с ключом -y. Удаление apparmor и его зависимостей отображено на рисунке 36

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 36 – Удаление apparmor и его зависимостей

Завершающим действием можно удалить пустые папки при помощи комонды: rm -rf /etc/apparmor /etc/apparmor.d. Удаление пустых папок отображено на рисунке 37



Рисунок 37 – Удаление пустых папок

КОНТРОЛЬНЫЕ ВОПРОСЫ

**1. Что такое eCryptfs? Где применяет? Какие алгоритмы шифрования поддерживает?**

eCryptfs (Enterprise Cryptographic File System) — это программа для шифрования файловой системы, которая предназначена для защиты данных. eCryptfs широко используется в Linux-системах для шифрования конфиденциальных данных на диске, например, в домашних каталогах пользователей или в облачных хранилищах. Алгоритмы шифрования, поддерживаемые eCryptfs, включают в себя AES

**2. Что такое LUKS? Где применяет? Какие алгоритмы шифрования поддерживает?**

LUKS (Linux Unified Key Setup) — это стандарт для шифрования дисков в операционных системах Linux. Он предоставляет прозрачное шифрование целых блочных устройств, таких как жесткие диски или разделы диска. LUKS используется для шифрования данных на уровне блочных устройств и обеспечивает высокий уровень безопасности. Он часто применяется для защиты конфиденциальных данных на ноутбуках, серверах или других устройствах. LUKS поддерживает различные алгоритмы шифрования, включая: AES, Twofish

**3. Что такое apparmor ? Какие правила могут быть использованны? С какими объектами работает apparmor?**

AppArmor (Application Armor) — это система безопасности для контроля доступа к файлам, директориям и другим ресурсам на уровне приложений в операционных системах Linux. Она позволяет определить правила доступа для конкретных приложений, ограничивая их возможности доступа к определенным ресурсам. Правила в AppArmor могут быть использованы для определения, какие файлы, директории и другие ресурсы могут быть доступны приложению. ppArmor работает с различными объектами, такими как исполняемые файлы приложений, библиотеки, конфигурационные файлы и другие ресурсы, к которым приложение может обращаться во время своей работы

ВЫВОД

В ходе выполнения лабораторной работы по теме: «Защита хоста» получили практический навык защиты хоста при эксплуатации СУБД