Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ОТЧЕТ

к лабораторной работе по дисциплине:

|  |
| --- |
| **Администрирование информационных систем** |
| Средства безопасности в Ubuntu Server |

наименование темы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Выполнил студент группы: | ИСМб-19-1 |  |  |  | Михейко Ю.А. |
|  |  | подпись |  | Фамилия И.О |
| Проверил: |  |  |  |  | Хритова М.А. |
|  | должность |  | подпись |  | Фамилия И.О |

Иркутск 2023 г.

Содержание

[Содержание 2](#_Toc128844256)

[1 Введение 3](#_Toc128844257)

[1 Основные меры и средства для обеспечения защиты сервера 4](#_Toc128844258)

[2 Средства безопасности в Ubuntu Server 5](#_Toc128844259)

[2.1 Управление пользователем 5](#_Toc128844260)

[2.1.1 Создание суперпользователя 5](#_Toc128844261)

[2.1.2 Создание пользователя 5](#_Toc128844262)

[2.1.3 Безопасность профиля пользователя 6](#_Toc128844263)

[2.1.4 Политика паролей 6](#_Toc128844264)

[2.1.5 Время жизни пароля 7](#_Toc128844265)

[2.2 Безопасность консоли 8](#_Toc128844266)

[2.3 Firewall 9](#_Toc128844267)

[2.3.1 Настройка ufw 9](#_Toc128844268)

[2.3.2 Интеграция приложений в ufw 9](#_Toc128844269)

[2.3.3 Маскировка IP 10](#_Toc128844270)

[2.3.3 Журналы 12](#_Toc128844271)

[2.4 AppArmor 12](#_Toc128844272)

[2.4.1 Установ ка apparmor-profiles 12](#_Toc128844273)

[2.4.2 Использование AppArmor 13](#_Toc128844274)

[2.4.3 Профили AppArmor 14](#_Toc128844275)

[3 Заключение 16](#_Toc128844276)

1 Введение

**Цель работы:** получить начальные навыки практического администрирования программных средств безопасности в операционной системе UbuntuServer, изучить управление пользователями, Firewall, AppArmor.

**Требования к отчетным документам:** Отчетный документ представляется в печатном или электронном виде, в форматах pdf, doc(x).

Отчет должен содержать следующие главы:

1. Введение.
2. Теоретическая часть. Основные меры и средства для обеспечения защиты сервера и сети от любого набора потенциальных угроз безопасности.
3. Практическая часть (привести использованные команды и скриншоты).

3.1. Управление пользователем. Определение суперпользователя, добавление и удаление пользователя. Безопасность профиля пользователя. Политика паролей.

3.2. Безопасность консоли.

3.3. Firewall. Настройка ufw. Интеграция приложений в ufw. Маскировка IP. Журналы.

3.4 AppArmor. Использование AppArmor. Профили.

1. Заключение (полученные результаты).

1 Основные меры и средства для обеспечения защиты сервера

Безопасность всегда должна учитываться, когда устанавливаются, разворачиваются и используются любые типы компьютерных систем. Хотя свежеустановленная Ubuntu сравнительно безопасна для немедленного использования в интернете, важно иметь сбалансированное понимание состояния безопасности ваших систем, исходя из их использования после развертывания.

Для обеспечения защиты создаются физические препятствия к проникновению злоумышленников к аппаратуре. Устанавливается контроль над всеми ресурсами системы. Криптографическое преобразование информации с целью маскировки проводится при передаче ее по линиям связи на большие расстояния. Заключительный этап – создание свода правил безопасности, принуждение всех сотрудников организации к их исполнению.

Главным образом обеспечение безопасности локальных сетей зависит от программных средств. К таковым относятся:

• Межсетевые экраны. Это промежуточные элементы компьютерной сети, которые служат для фильтрации входящего и исходящего трафика. Риск несанкционированного доступа к информации становится меньше.

• Прокси-серверы. Производят ограничение маршрутизации между глобальной и локальной частями сети.

• VPN. Позволяют передавать информацию по зашифрованным каналам.

• Разные наборы протоколов, которые нужны для создания защищенного соединения и установления контроля над элементами локальной сети.

Эти приложения, встроенные в оперативную систему и специализированные, шифруют данные. Данные разграничивают потоки информации.

К средствам физической защиты относят систему архивирования и размножения информации. Для крупномасштабных корпоративных сетей рекомендовано организовывать отдельный архивационный сервер.

Разумеется, наиболее надежными считаются комплексные способы защиты компьютерных сетей, сочетающие в себе набор мер безопасности, и чем их больше, тем лучше. В данном случае специалисты наряду с обеспечением стандартных решений разрабатывают специальные планы действий на случай возникновения нештатных ситуаций.

2 Средства безопасности в Ubuntu Server

2.1 Управление пользователем

2.1.1 Создание суперпользователя

Для полноценного использования операционной системы был настроен root-пользователь. Для задания пароля root была использована команда sudo passwd.

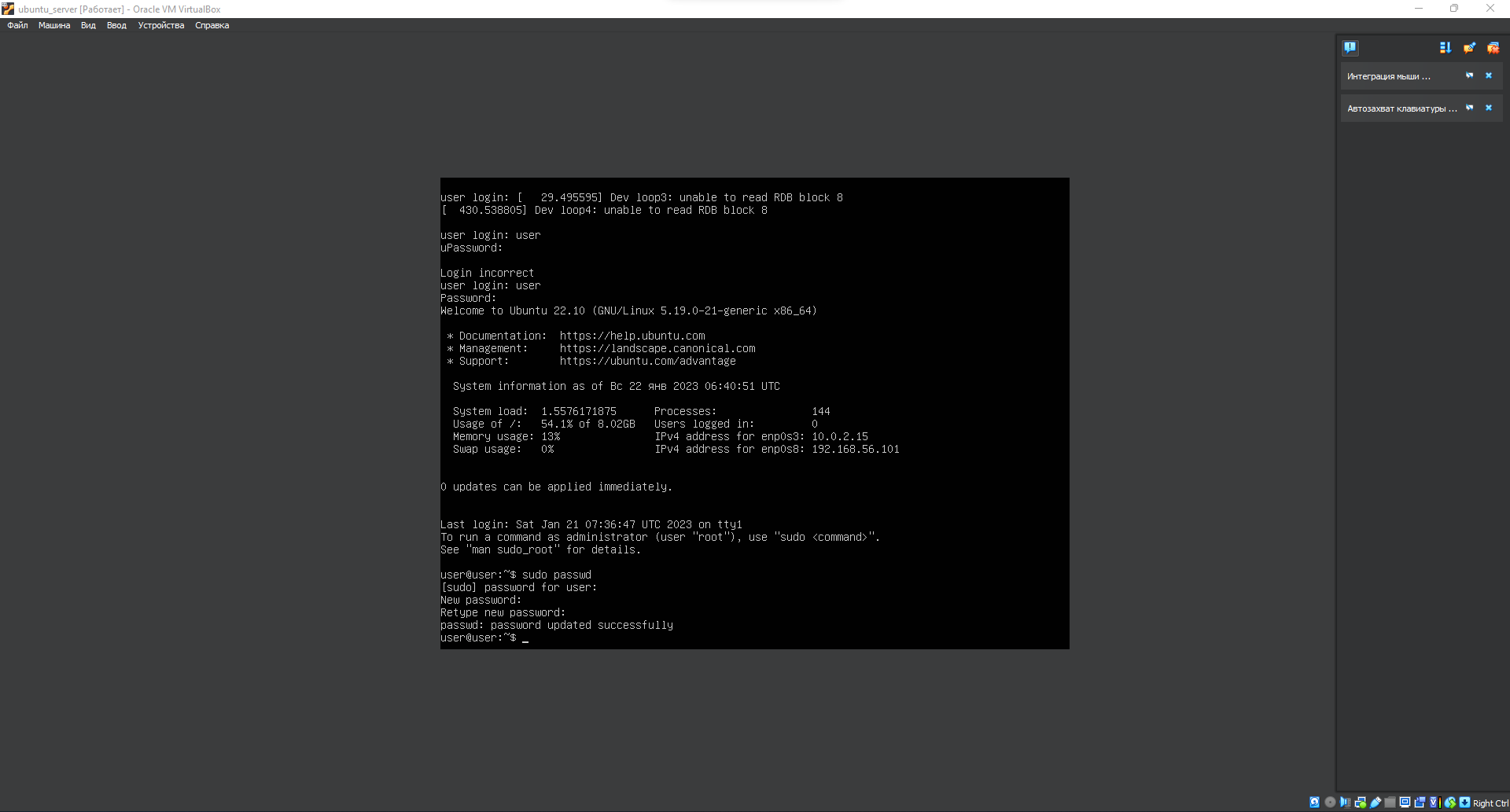


Рисунок 1 – Задание пароля суперпользователя

2.1.2 Создание пользователя

Для добавления учетной записи пользователя используется команда sudo adduser «username», указывается пароль и дополнительная информация о пользователе. Указание дополнительной информации является обязательной, поэтому данные поля можно оставить пустыми.

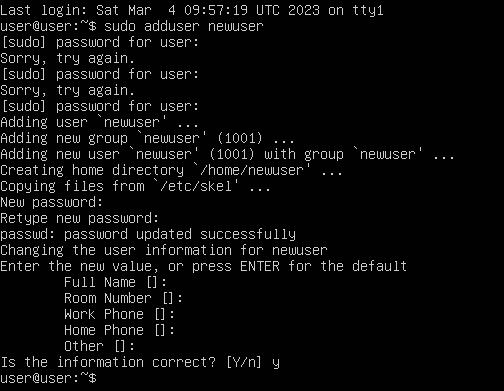


Рисунок 2 – Создание нового пользователя

Для просмотра списка всех существующих пользователей можно воспользоваться командой cut -d: -f1 /etc/passwd.

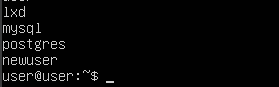


Рисунок 3 – Просмотр списка пользователей

Для удаления пользователя и его первичной группы, используется команда sudo deluser newuser.

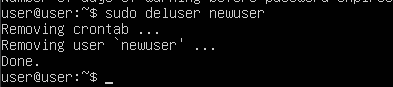


Рисунок 4 – Удаление пользователя

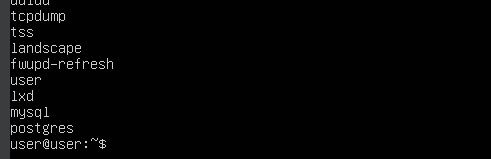


Рисунок 5 – Просмотр списка пользователей после удаления

2.1.3 Безопасность профиля пользователя

Когда создается новый пользователь, утилита adduser создает новый именной каталог /home/"username". Профиль по умолчанию формируется по содержимому, находящемуся в каталоге /etc/skel, который включает все основы для формирования профилей.

По умолчанию пользовательские домашние каталоги создаются с правами чтения/выполнения для всех. Это означает, что все пользователи просматривать и получать доступ к содержимому других домашних каталогов, поэтому нужно уделять внимание правам доступа на пользовательские домашние каталоги для поддержания конфиденциальности.

Для проверки прав доступа на домашние каталоги существующих пользователей используется команда ls -ld /home/username.



Рисунок 6 – Проверка прав доступа

Чтобы удалить права чтения для всех, используем команду sudo chmod 0750 /home/username.

2.1.4 Политика паролей

Строгая политика паролей – один из наиболее важных аспектов подхода к безопасности. По умолчанию Ubuntu требует минимальную длину пароля в 6 символов, также, как и некоторые основные проверки на разброс значений. Эти параметры управляются файлом /etc/pam.d/common-password. Для доступа к данному файлу необходимо применить команду sudo nano /etc/pam.d/common-password.

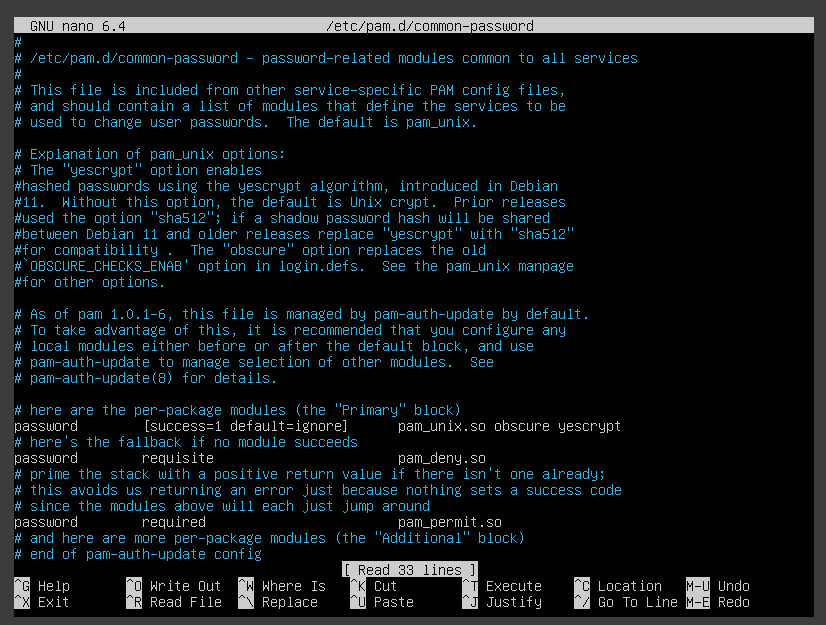


Рисунок 7 – Файл common-password

Для того, чтобы установить минимальную длину пароля в 8 символов, необходимо дописать в конце переменной password [success=1 default=ignore] pam\_unix.so obscure yescrypt min=8.

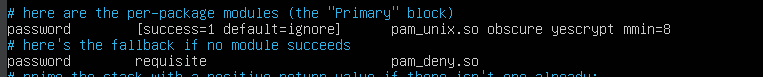


Рисунок 8 – Изменение файла common-password

Базовые проверки на качество и минимальную длину пароля не применяются к администратору, использующего команды уровня sudo для настройки нового пользователя.

2.1.5 Время жизни пароля

При создании учетных записей пользователей возможно создать политику минимального и максимального времени жизни пароля чтобы заставлять пользователей менять их пароли по истечении определенного времени.

Для простого просмотра текущего статуса учетной записи пользователя используется команда sudo chage -l newuser.

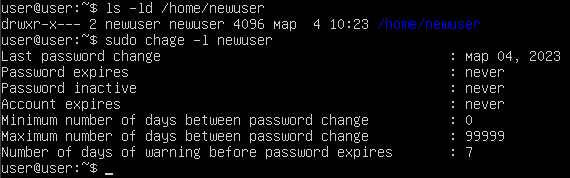


Рисунок 9 – Просмотр статуса учетной записи

Результат данной команды демонстрирует отсутствие каких-либо применённых политик.

Для изменения параметров учетной записи необходимо применить команду sudo chage testuser.

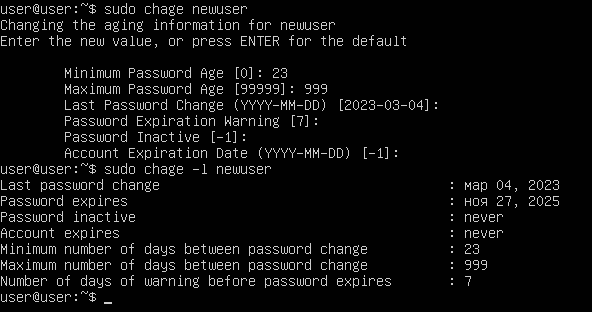


Рисунок 10 – Просмотр статуса учетной записи после редактирования

2.2 Безопасность консоли

Безопасность консоли стоит рассматривать просто как один из компонентов общей физической безопасности. Блокируемая "ширма" (screen door) может защитить от случайного криминала и очень сильно замедлить активное воздействие, поэтому очень желательно соблюдать простейшие предосторожности по отношению к безопасности консоли.

Для начала необходимо отключить сочетание Ctrl+Alt+Delete, так как любой пользователь, имеющий физический доступ к клавиатуре может просто нажать данную комбинацию клавиш для перезагрузки сервера без необходимости входить в систему. Для этого необходимо использовать следующие команды:

sudo systemctl mask ctrl-alt-del.target

sudo systemctl daemon-reload



Рисунок 11 – Отключение сочетания клавиш

2.3 Firewall

2.3.1 Настройка ufw

Инструмент для настройки сетевой защиты Ubuntu по умолчанию – это ufw. Он разработан для легкой настройки iptables и предоставляет дружественный способ создания сетевой защиты для IPv4 и IPv6.

По умолчанию ufw отключен, чтобы включить необходимо ввести в терминале команду sudo ufw enable.



Рисунок 12 – Включение утилиты ufw

Для выключения используется команда sudo ufw disable.



Рисунок 13 – Отключение утилиты ufw

Принципы работы ufw таковы: входящие и исходящие пакеты проверяются на предмет соответствия имеющимся правилам фильтрации, после чего выполняется действие, установленное для этого правила. Если подходящее правило не будет найдено, используется действие, установленное по умолчанию

Для сброса всех настроек и возврата firewall к изначальному состоянию применяется команда sudo ufw reset.



Рисунок 14 – Сброс утилиты ufw

2.3.2 Интеграция приложений в ufw

Приложения, которые открывают порты, можно включать в профили ufw, они детализируют какие порты необходимы этому приложению для корректной работы. Профили содержатся в /etc/ufw/applications.d, и могут быть отредактированы, если порты по умолчанию были изменены.

Для того, чтобы посмотреть для каких приложений установлен профиль необходимо применить команду sudo ufw app list.

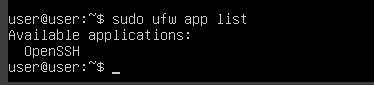


Рисунок 15 – Просмотр списка приложений интегрированных с ufw

разрешить трафик по порту, используя профиль приложения, можно командой sudo ufw allow OpenSSH.

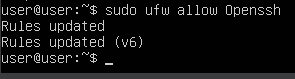


Рисунок 16 – Разрешение работы с трафиком

Для просмотра деталей какие порты, протоколы и прочее определены для приложения используется команда sudo ufw app info OpenSSH.



Рисунок 17 – Проверка порта, используемого приложением

2.3.3 Маскировка IP

Цель маскировки ip-адреса состоит в том, чтобы компьютеры с частными, не маршрутизируемыми ip-адресами в сети могли иметь доступ к Интернету через компьютер, выполняющий маскировку. Трафик из частной сети, попадающий в Интернет, должен быть правильно выпущен для корректного ответа, отправленного именно тому компьютеру, который послал запрос.

Маскировка ip-адреса может быть достигнута с использованием различных правил ufw. Это возможно благодаря дополнению к ufw, которым является iptables-restore с файлами правил, расположенных в /etc/ufw/\*.rules. Эти файлы являются отличным способом для добавления правил в iptables без использования ufw.

Для начала необходимо активировать перенаправление в ufw, изменив конфигурацию двух файлов. В первом файле /etc/default/ufw необходимо изменить значение в строке DEFAULT\_FORWARD\_POLICY на “ACCEPT”.

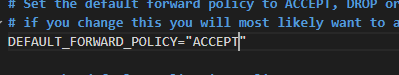


Рисунок 18 – Редактирование файла ufw

Во втором файле /etc/ufw/sysctl.conf, изменить: net/ipv4/ip\_forward=1. Аналогично для IPv6: net/ipv6/conf/default/forwarding=1.

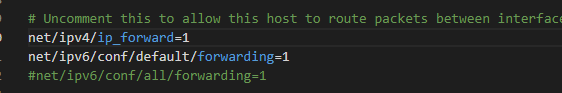


Рисунок 19 – Редактирование файла sysctl.conf

Далее необходимо добавить правила в файл /etc/ufw/before.rules. Правила по умолчанию описаны лишь в таблице filter, для работы маскировки нужно отредактировать таблицу nat, добавив следующие строки в начало файла конфигурации сразу после заголовка с комментарием

# nat Table rules

\*nat

:POSTROUTING ACCEPT [0:0]

# Forward traffic from eth1 through eth0.

-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

# don't delete the 'COMMIT' line or these nat table rules won't be processed

COMMIT

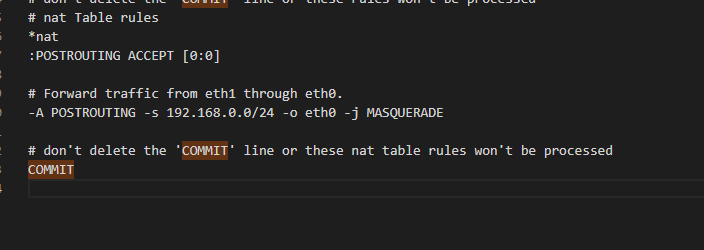


Рисунок 20 – Редактирование файла before.rules

Далее необходимо выключить и повторно включить ufw для применения изменений командой sudo ufw disable && sudo ufw enable. IP маскировка теперь должна быть включена.

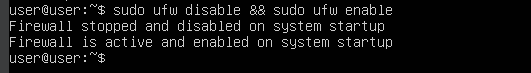


Рисунок 21 – Перезапуск ufw

2.3.3 Журналы

Firewall крайне необходимы для обнаружения атак, возникающих проблем с правилами, а также обнаружения повышенной активности в сети. В настройках firewall необходимо включить журналирование для правил, которое должно быть указано перед списком правил (правил, которые решают дальнейшую судьбу пакета, такие как ACCEPT, DROP или REJECT).

При использовании ufw журналирование можно включить командой sudo ufw logging on.

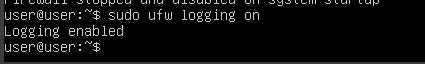


Рисунок 22 – Включение журналирования

Для выключения журналирования используется команда sudo ufw logging off.



Рисунок 23 – Выключение журналирования

2.4 AppArmor

2.4.1 Установка apparmor-profiles

AppArmor – это реализация Модуля безопасности Linux по управлению доступом на основе имен. Он устанавливается и загружается по умолчанию. Принцип работы Apparmor: модуль использует профили приложений для определения какие файлы и права доступа требуются приложению, поэтому необязательно полностью включать или отключать Apparmor, можно контролировать доступ только для отдельных приложений. Некоторые пакеты устанавливают свои собственные профили, а дополнительные профили можно найти в пакете apparmor-profiles.

Для того, чтобы установить пакет apparmor-profiles, выполняется команда sudo apt-get install apparmor-utils apparmor-profiles.

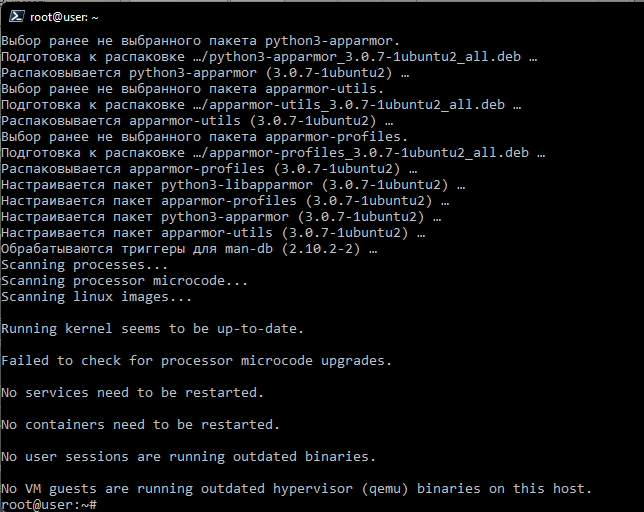


Рисунок 24 – Установка пакета apparmor-profiles

Профили AppArmor имеют два режима выполнения:

1. Фиксации/Обучения (complain): нарушения профиля разрешаются и сохраняются в журнале. Полезно для тестирования и разработки новых профилей

2. Предписаний/Ограничений (enforce): принуждает следовать политике профиля, при этом также записывает нарушения в журнал.

2.4.2 Использование AppArmor

Пакет apparmor-utils содержит утилиты командной строки, которые можно использовать для изменения режима выполнения AppArmor, поиска статуса профиля, создания новых профилей и другой функционал. Основными командами являются:

• apparmor\_status. Используется для просмотра текущего статуса профиля AppArmor.

• aa-complain. Переводит профиль в режим обучения.

• aa-enforce. Переводит профиль в режим ограничений.

Проверка статуса утилит осуществляется командой sudo apparmor\_status.

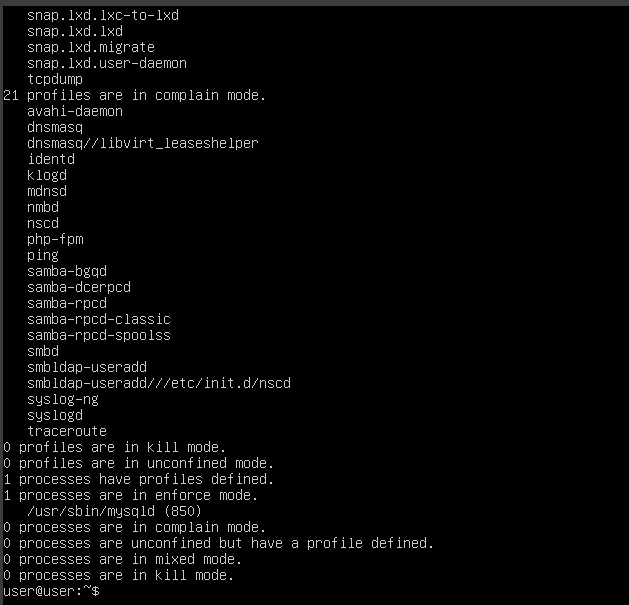


Рисунок 25 – Проверка статуса утилит

aa-complain переводит профиль в режим обучения (complain). sudo aa-complain /path/to/bin

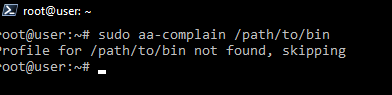


Рисунок 26 – Перевод профиля в режим обучения

aa-enforce переводит профиль в режим ограничений (enforce). sudo aa-enforce /path/to/bin

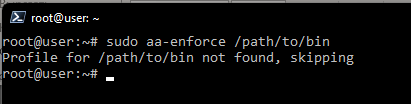


Рисунок 27 – Перевод профиля в режим ограничений

2.4.3 Профили AppArmor

Профили AppArmor – это простые текстовые файлы, которые расположены в /etc/apparmor.d/. Файлы профиля называются соответственно полному пути до исполняемого файла, которым они управляют, с заменой символа «/» на «.». Например, /etc/apparmor.d/bin.ping — это профиль AppArmor для команды /bin/ping. Существует два основных типа правил, используемых в профиле:

1. Записи путей (Path entries): которые описывают к каким файлам приложение имеет доступ в файловой системе.

2. Записи разрешений (Capability entries): определяют какие права ограничиваемый процесс имеет право использовать

В качестве примера продемонстрирован /etc/apparmor.d/bin.ping с помощью команды sudo nano /etc/apparmor.d/bin.ping

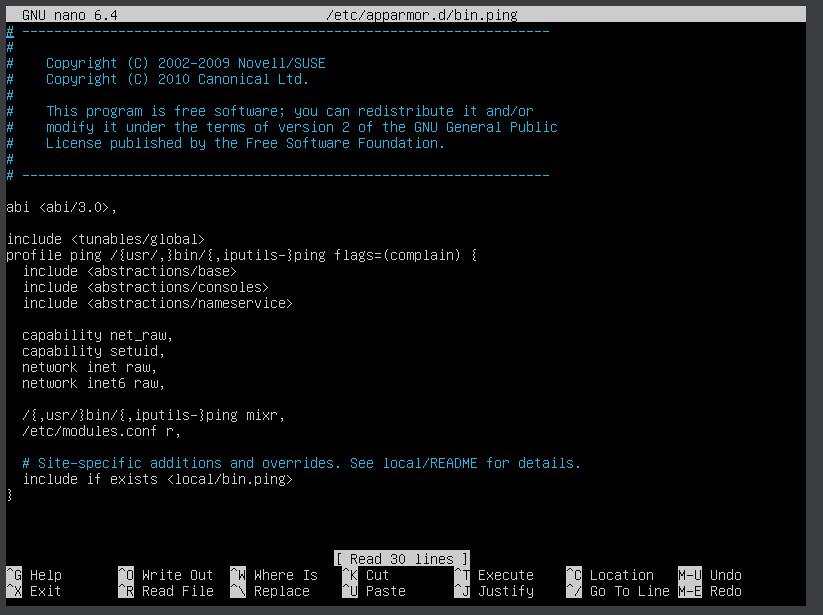


Рисунок 28 – Файл /etc/apparmor.d/bin.ping

C помощью команды aa-genprof возможно создать новый профиль.

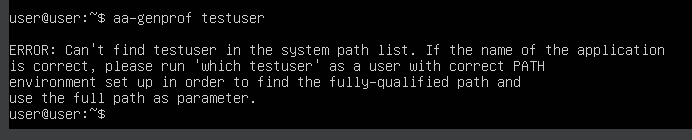


Рисунок 29 – Создание нового профиля

Дополнительно программа aa-logprof может быть использована для сканирования файлов журнала AppArmor для проверки сообщений, их рассмотрения (анализа) и обновления профилей.

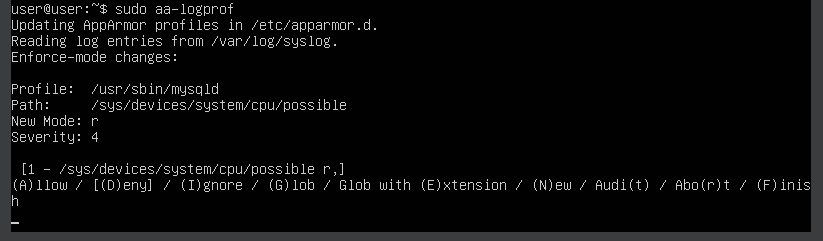


Рисунок 30 – Сканирование файлов журнала

3 Заключение

В результате выполнения лабораторной работы были получены навыки практического использования функционала суперпользователя, изучены средства управления пользователем, произведена соответствующая настройка.

Дополнительно проведено ознакомление с функционалом утилит Firewall и AppArmor.