Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

**ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

Институт информационных технологий и

анализа данных

|  |
| --- |
| наименование института |
| **Отчет** по лабораторной работе №4  по дисциплине «Администрирование информационных систем»  «Средства безопасности в Ubuntu Server» | | |  |

наименование темы

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | |
| Выполнили студенты |  | ИСМб-18-1 | |  |  |  | И. Г. Михайлов |
| Проверил |  | шифр группы | |  | подпись |  | И.О. Фамилия  М.А. Хритова |
|  |  |  | |  | подпись |  | И.О. Фамилия |
|  | | |  | |  | | |

Иркутск 2020 г.

**Содержание**

[Введение 3](#_Toc57311653)

[1 Теоретическая часть 4](#_Toc57311654)

[1.1 Основные меры и средства для обеспечения защиты сервера и сети от любого набора потенциальных угроз безопасности 4](#_Toc57311655)

[2 Практическая часть 5](#_Toc57311656)

[2.1 Управление пользователем 5](#_Toc57311657)

[2.2 Безопасность консоли 8](#_Toc57311658)

[2.3 Firewall 9](#_Toc57311659)

[2.4 AppArmor 14](#_Toc57311660)

[Заключение 19](#_Toc57311661)

Введение

Целью данной лабораторной работы является получение начальных навыков практического администрирования программных средств безопасности в операционной системе UbuntuServer, изучить управление пользователями, Firewall, AppArmor.

**Задание:**

1. Изучить информацию по ссылке

http://help.ubuntu.ru/wiki/руководство\_по\_ubuntu\_server/безопасность

2. Протестировать средства управления пользователями.

3. Изучить средства обеспечения безопасности консоли.

4. Настроить Firewall.

5. Настроить AppArmor.

6. Написать отчет.

1 Теоретическая часть

1.1 Основные меры и средства для обеспечения защиты сервера и сети от любого набора потенциальных угроз безопасности

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 Практическая часть

2.1 Управление пользователем

Управление пользователями является важной частью безопасности системы. Неэффективные пользователи и управление привилегиями часто приводят множество систем к компрометации. Поэтому важно понимать, как защитить ваш сервер с помощью простых и эффективных методик управления пользовательскими учетными записями.

Суперпользователь – применение пользователями инструмента с именем sudo для переноса административных обязанностей. Sudo позволяет авторизованным пользователям временно повышать их привилегии, используя их собственный пароль вместо знания пароля, присвоенного суперпользователю.

Теперь выполним некоторые команды от имени суперпользователя. Для того, чтобы разрешить учетную запись суперпользователя, установим ей пароль, используя команду «sudo passwd». На рисунке 1 мы видим, что новый пароль успешно установлен.

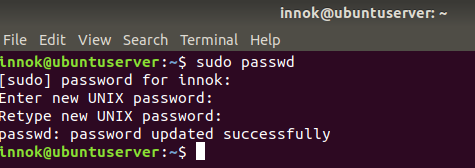


Рисунок 1 – Установка пароля

Добавление и удаление пользователей.

Для добавления учетной записи пользователя используем команду sudo adduser «username», указываем пароль и дополнительную информацию о пользователе (рис. 2). Это не обязательно, поэтому можно оставить поля пустыми.

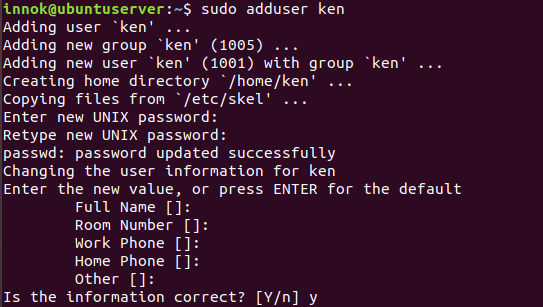


Рисунок 2 –Добавление пользователя

Для удаления пользователя и его первичной группы, используем команду «sudo deluser ken» (рис. 3)

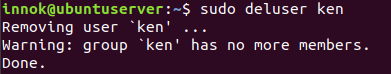


Рисунок 3 – Удаление пользователя

Удаление пользователя не удаляет связанный с ним домашний каталог. Оставлено на ваше усмотрение хотите ли вы удалить каталог вручную или оставите его в соответствии с вашими политиками хранения.

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 используем команду «ls -ld /home/username». На рисунке 4 видно, что каталог /home/ken имеет доступ на чтение для всех.



Рисунок 4 – Проверка прав доступа

Чтобы удалить права чтения для всех, используем команду «sudo chmod 0750 /home/username». Другой, более эффективный способ заключается в изменении глобальных прав доступа по умолчанию для adduser при создании домашних каталогов. Для этого необходимо отредактировать файл /etc/adduser.conf, изменив переменную DIR\_MODE на что-то более подходящее, после чего все новые домашние каталоги будут получать корректные права доступа, например, DIR\_MODE=0750 (рис. 5).

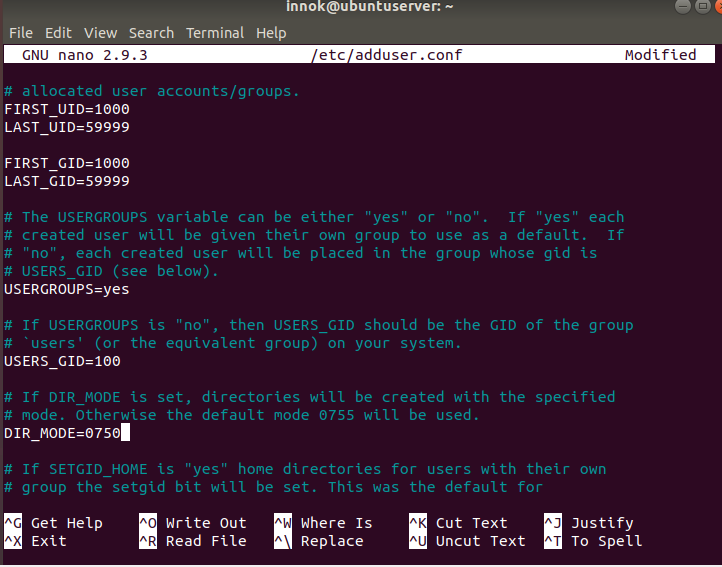


Рисунок 5 – Удаление пользователя

После исправления прав доступа проверим результаты используя команду «ls -ld /home/ken». На рисунке 6, видим, что права на чтение для всех удалены.



Рисунок 6 – Удаление прав

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, открываем его и редактируем как нам надо.

Для того, чтобы установить минимальную длину пароля в 8 символов, допишем в конце переменной «password [success=2 default=ignore] pam\_unix.so obscure sha512» min=8 (рис.7).

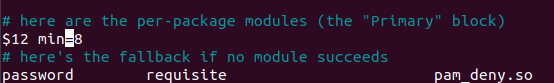


Рисунок 7 – Файл /etc/pam.d/common-password

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

Время жизни пароля.

При создании учетных записей пользователей мы должны 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 введем следующую команду sudo chage -l ken (рис. 8), после ввода команды мы можем увидеть, что нет никаких применённых политик.

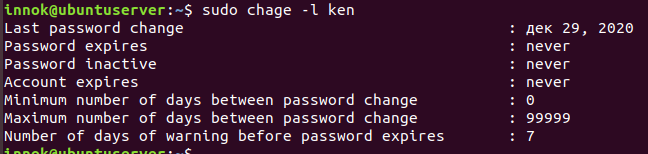


Рисунок 8 – Текущий статус учетной записи

Для установки этих значений просто используем следующую команду, следуя интерактивным подсказкам (рис. 9). Также на рисунке 9 мы видим, что настройка была применена.

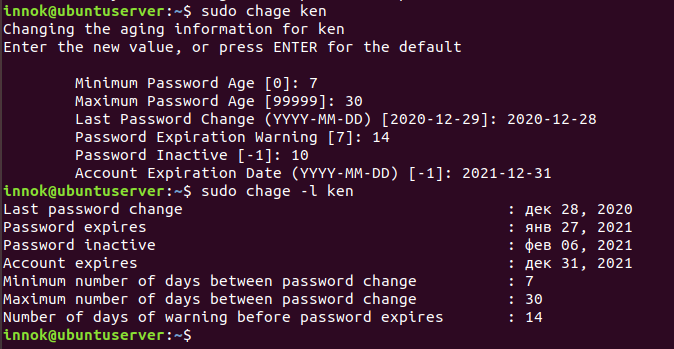
s

Рисунок 9 – Настройка политики паролей

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 отключим 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 откроем файл /etc/init/control-alt-delete.conf и закомментируем строку #exec shutdown -r now "Control-Alt-Delete pressed" (рис. 10).

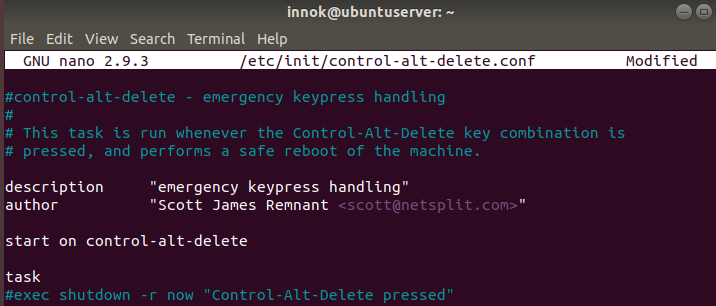


Рисунок 10 – Отключение Ctrl+Alt+Delete

2.3 Firewall

Ядро линукс включает подсистему Netfilter, который используется для манипулирования или решения судьбы сетевого трафика, передаваемого в или через ваш сервер. Все современные решения линукс по сетевой защите используют эту систему пакетной фильтрации.

Система пакетной фильтрации на уровне ядра была бы малоиспользуемая администраторами без пользовательского интерфейса для ее управления. Для этого предназначен iptables. Когда пакет попадает на ваш сервер, он передается подсистеме Netfilter для одобрения, изменения или отказа на основе правил, которые она получает от интерфейса пользователя через iptables. Таким образом iptables — это все, что вам нужно для управления вашей сетевой защитой, если вы хорошо с ним знакомы, однако множество внешних интерфейсов доступны для упрощения этой задачи.

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.

Настройка ufw.

По умолчанию ufw отключен, чтобы включить его, набираем в терминале команду «sudo ufw enable» (рис. 11), а для выключения «sudo ufw disable» (рис. 12).



Рисунок 11 – Команда для включения ufw



Рисунок 12 – Выключение защиты

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

После включения ufw необходимо открыть SSH порт с помощью команды «sudo ufw allow 22» (рис. 13), где 22 – это номер порта. Это нужно для того, чтобы создать правила, прямо разрешающие входящие соединения (например, SSH или HTTP), так как, если мы сейчас активируем брандмауэр ufw, все входящие соединения будут запрещены. Соединение SSH предназначено для использования облачного сервера, чтобы можно было подключаться к серверу и управлять им.

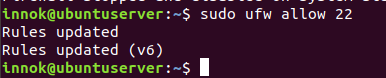


Рисунок 13 – Открытие SSH порта

Для просмотра, какие правила используются в данный момент, используются команда «sudo ufw status» и команда «sudo ufw status verbose» для полной информации. На рисунке 14 представлен результат работы данной команды, и мы видим, что межсетевой экран активен и создано правило, которое отменяет запрет входящего трафика для порта 22.

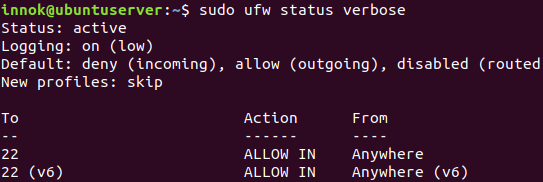


Рисунок 14 – Результат команды «sudo ufw status verbose»

Для закрытия порта используется команда deny, для удаления delete deny. Чтобы разрешить другие соединения, например, HTTP на порту 80, используется команда allow http или allow 80. Аналогично для соединения HTTPS на порту 443. Отличие этих портов в том, что HTTPS используется веб-серверами c шифрованием, а HTTP без.

Последняя команда, которую мы рассмотрим - «sudo ufw reset» (рис. 15). Она используется для сброса всех настроек и возвращает фаервол к изначальному состоянию. Для подтверждения нажимаем «y», после чего все правила будут удалены, а ufw – выключен, так как по умолчанию он находится именно в таком состоянии. Это команда может быть очень полезна для исправления положения в процессе неправильной настройки.

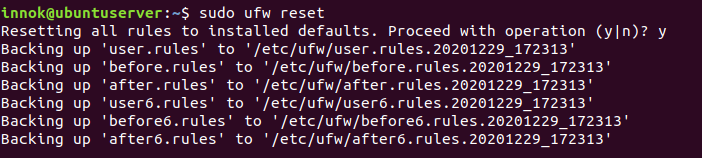


Рисунок 15 – Результат команды «sudo ufw reset»

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 введем команду «sudo ufw app list» (рис. 16).

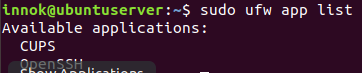


Рисунок 16 – Приложения с ufw

Аналогично, разрешить трафик по порту, используя профиль приложения, можно командой «sudo ufw allow CUPS» (рис. 17).



Рисунок 17 – Разрешение трафика

Для просмотра деталей какие порты, протоколы и прочее определены для приложения введем команду «sudo ufw app info CUPS» (рис. 18).

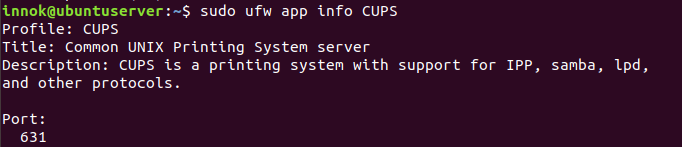


Рисунок 18 – Детали приложения

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.

Чтобы сделать это, ядро модифицирует заголовок каждого пакета так, чтобы ответ приходил нужному компьютеру, а не частному ip-адресу, который послал запрос, что невозможно в рамках сети Интернет. Линукс использует Трассировку Соединений (conntrack) для трассировки каждого из соединений, принадлежащих соответствующим компьютерам, и перенаправляет каждый возвращенный пакет. Трафик, покидает астную сеть «маскируясь» таким образом, будто исходит от шлюза Ubuntu. Этот процесс обозначен в документации Microsoft как Internet Connection Sharing (Общий доступ к Интернет-Соединению).

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 активируем перенаправление в ufw, изменим конфигурацию двух файлов. Первый откроем файл /etc/default/ufw и изменим значение в строке DEFAULT\_FORWARD\_POLICY на “ACCEPT” (рис. 19). Затем файл /etc/ufw/sysctl.conf, так: net/ipv4/ip\_forward=1. Аналогично для IPv6: net/ipv6/conf/default/forwarding=1(рис. 20)

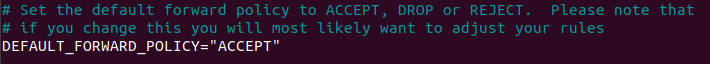


Рисунок 19 – Редактирование файла /etc/default/ufw



Рисунок 20 – Редактирование файла/etc/ufw/sysctl.conf

Теперь добавим правила в файл /etc/ufw/before.rules. Правила по умолчанию описаны лишь в таблице filter, а для работы маскировки нам нужно отредактировать таблицу nat. Добавим следующие строки в начало файла конфигурации сразу после заголовка с комментарием (рис. 21).

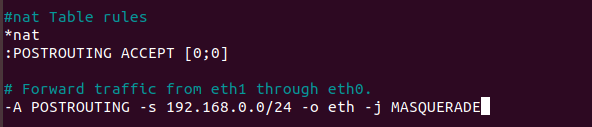


Рисунок 21 – Редактирование файла/etc/ufw/before.rules

Также при изменении каких-либо rules файлов в каталоге /etc/ufw, нужно убедиться, что данные строки являются последними для каждой измененной таблицы: # don't delete the 'COMMIT' line or these rules won't be processed

COMMIT

Наконец, выключим и повторно включим ufw для применения изменений командой «sudo ufw disable && sudo ufw enable» (рис. 22). IP маскировка теперь должна быть включена.



Рисунок 22 – Отключение и включение ufw

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», а, чтобы выключить заменить значение on на off (рис. 23).

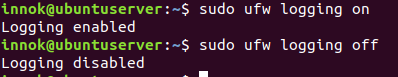


Рисунок 23 – Включение и отключение журналирования

Для iptables:

sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 \

-j LOG --log-prefix "NEW\_HTTP\_CONN: "

В этом случае в начале поступит запрос на порт 80 от компьютера в локальной сети, затем будет сгенерирован файл журнала в dmesg который выгдлядит примерно так (одна строка разделена на три для корректного отображения на экране):

[4304885.870000] NEW\_HTTP\_CONN: IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00

SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP

SPT=53981 DPT=80 WINDOW=32767 RES=0x00 SYN URGP=0

Этот текст журнала также появится в файле /var/log/messages, /var/log/syslog и /var/log/kern.log. Данные настройки можно изменить, отредактировав файл /etc/syslog.conf аналогично или при установке и настройке ulogd, а также используя ULOG вместо LOG, ulogd – это пользовательский сервер, который слушает инструкции ядра для дальнейшего журналирования, в частности для firewall, и может вести журналирование даже в PostgreSQL или MySQL базы данных. Для того, чтобы легко разобраться в файлах журнала можно использовать их анализаторы, такие как logwatch, fwanalog, fwlogwatch или lire.

2.4 AppArmor

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, выполняем команду «sudo apt-get install apparmor-utils apparmor-profiles», затем подтверждаем операцию. Выполнение команды показано на рисунке 24.

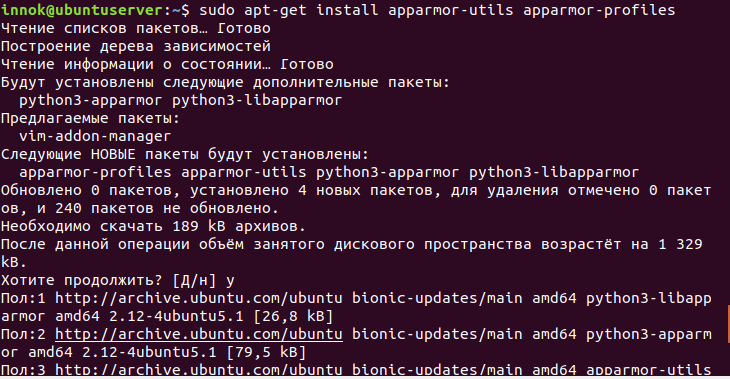


Рисунок 24 – Результат команды «sudo apt-get install apparmor-utils»

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.

Использование AppArmor.

Пакет apparmor-utils содержит утилиты командной строки, которые можно использовать для изменения режима выполнения AppArmor, поиска статуса профиля, создания новых профилей и т.п.. Рассмотрим основные команды:

* apparmor\_status. Используется для просмотра текущего статуса профиля AppArmor.
* aa-complain. Переводит профиль в режим обучения. (рис. 26)
* aa-enforce. Переводит профиль в режим ограничений. (рис. 27)

После установки пакета утилит проверили статус профиля. На рисунке 25 видно, что загружено 71 профилей, 34 из которых в режиме ограничений, 37 в режиме обучения.

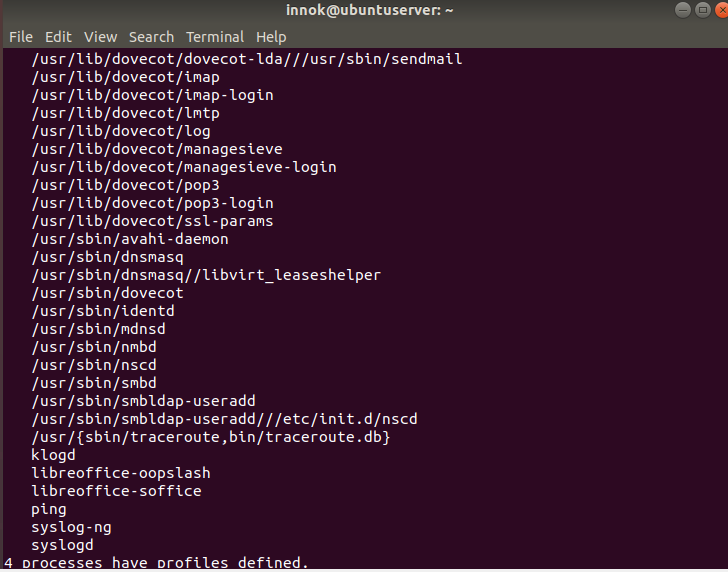


Рисунок 25 – Статус профиля Apparmor



Рисунок 26 – Перевод профиля в режим обучения



Рисунок 27 – Перевод профиля в режим ограничений

Профили AppArmor расположены в каталоге /etc/apparmor.d. Его можно использовать для управления режимом всех профилей. Для перевода всех профилей в режим обучения используется команда «sudo aa-complain /etc/apparmor.d/\*», а для режима ограничений: «sudo aa-enforce /etc/apparmor.d/\*».

Команда apparmor\_parser используется для загрузки профиля в ядро. Она также может использоваться для повторной загрузки загруженного профиля при использовании опции '-r'. Для загрузки используется команда «cat /etc/apparmor.d/profile.name | sudo apparmor\_parser –a», для перезагрузки: «cat /etc/apparmor.d/profile.name | sudo apparmor\_parser –r».

Директория /etc/apparmor.d/disable может использоваться совместно с опцией apparmor\_parser -R для отключения профиля. Для активации отключенного профиля необходимо удалить символическую ссылку на профиль в /etc/apparmor.d/disable/ и загрузить профиль используя опцию '-a'.

Чтобы отключить AppArmor, вводим команду «sudo /etc/init.d/apparmor stop». Для повторной активации AppArmor – команда «sudo /etc/init.d/apparmor start».

Профили.

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 посмотрим /etc/apparmor.d/bin.ping: (рис. 28)

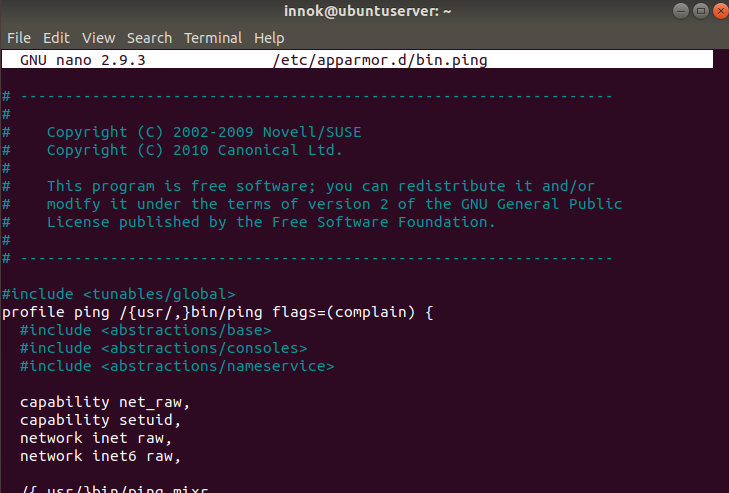


Рисунок 28 – /etc/apparmor.d/bin.ping

Создание профиля

1. Разработка плана тестирования: Попробуйте подумать о том, как приложение будет выполняться. План тестирования стоит разделить на маленькие тестовые блоки. Каждый тестовый блок должен иметь краткое описание и перечень шагов выполнения. Некоторые стандартные тестовые блоки:
   1. Запуск программы.
   2. Остановка программы.
   3. Перезагрузка программы.
   4. Тестирование всех команд, поддерживаемых сценарием инициализации.

2. Создание нового профиля: Используйте aa-genprof для создания нового профиля.

Команда в терминале: (рис. 29).

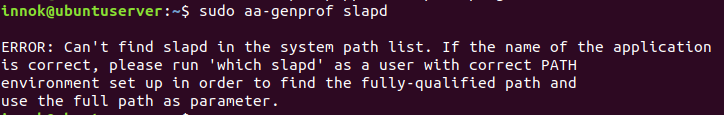


Рисунок 29 – Создание нового профиля

Обновление профилей.

Когда программа ведет себя неправильно, проанализируйте сообщения, отправленные в файлы журналов. Программа aa-logprof может быть использована для сканирования файлов журнала AppArmor для проверки сообщений, их рассмотрения (анализа) и обновления профилей. Команда в терминале: (рис. 30)

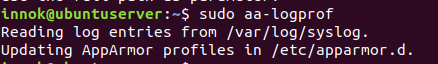


Рисунок 30 – Сканирование файлов журнала

Заключение

В данной лабораторной работе мы познакомились с понятием суперпользователь, изучили средства управления пользователя, провели настройки.

Так же мы познакомились и настроили с Firewal, а именно изучили инструмент настройки сетевой защиты ufw. Еще был изучен и настроен AppArmor.