ЛАБОРАТОРНАЯ РАБОТА № 4
«БРАНДМАУЭР UFW»

1. ЦЕЛЬ РАБОТЫ: Изучить основные сведения о брандмауэрах, их типы и организацию. Исследовать основные возможности работы с брандмауэром при помощи утилиты UFW.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Основные сведения о брандмауэрах

Для защиты локальной сети используется комплекс программного обеспечения, известный как Firewall (брандмауэр), или межсетевой экран. Брандмауэр позволяет "отгородить" систему или сеть от внешней сети. Он используется для предотвращения получения посторонними данных или ресурсов защищаемой сети, а также для контроля внешних ресурсов, к которым имеют доступ пользователи данной сети.

Чаще всего брандмауэр – это набор программ маршрутизации и фильтрации сетевых пакетов. Такие программы позволяют определить, можно ли пропустить данный пакет и если можно, то отправить его точно по назначению. Для того чтобы брандмауэр мог это сделать, ему необходимо определить набор правил фильтрации. Главная цель брандмауэра – контроль удаленного доступа извне или изнутри защищаемой сети или компьютера.

Брандмауэр позволяет лишь частично решить проблемы, связанные с обеспечением безопасного функционирования сети. Как бы хорошо он ни был настроен, если вовремя не обновить программный пакет, в котором была найдена уязвимость, или кто-то узнал логин и пароль пользователя сети или компьютера

– высока вероятность несанкционированного доступа. Основная задача брандмауэра – разрешать функционирование только тем службам, которым было разрешено работать в данной сети или защищаемом компьютере.

Брандмауэры можно разделить по типу построения защиты:

- пороговый брандмауэр и его разновидность бастионного типа;
- брандмауэр, организующий так называемую демилитаризованную зону.

Брандмауэр порогового типа призван защитить локальную сеть от атак извне, а при соответствующей настройке и от атак изнутри. Такого типа брандмауэры обычно используются для защиты небольшой сети или одного компьютера. Как правило, сетевые службы, предоставляющие услуги вне локальной сети (HTTP, FTP и т. п.), размещаются на том же компьютере, что и брандмауэр.

Организация демилитаризованной зоны оправдана тогда, когда в сети выделено несколько специальных компьютеров для интернет-сервисов, предоставляемых внешней сети, а также при отсутствии уверенности в благонадежности сотрудников. Для организации демилитаризованной зоны используются, по меньшей мере, два брандмауэра: один для защиты демилитаризованной зоны от проникновения извне, а второй – от проникновения из вашей собственной локальной сети. Организация демилитаризованной зоны сложнее, чем организация брандмауэра бастионного типа, но при этом обеспечивается большая защита данных.

Брандмауэр с фильтрацией пакетов

Брандмауэр с фильтрацией пакетов представляет собой "сито" для проходящих через него входящих и исходящих пакетов. В операционной системе Linux реализован брандмауэр, позволяющий контролировать ICMP-, UDP-и TCP-пакеты. Брандмауэр с фильтрацией пакетов организован как механизм, реализующий набор разрешающих и запрещающих правил для входящих и

исходящих пакетов. Этот набор правил определяет, какие пакеты могут проходить через конкретный сетевой интерфейс.

Брандмауэр с фильтрацией пакетов может производить с проходящим пакетом всего три действия:

1. переслать пакет в узел назначения;

2. удалить пакет без уведомления посылающей пакет стороны;

3. вернуть передающему компьютеру сообщение об ошибке.

Несмотря на простоту таких действий, в большинстве случаев их достаточно для организации эффективной защиты.

Как правило, брандмауэр устанавливается для того, чтобы контролировать данные, которыми компьютеры обмениваются с Интернетом. В результате работы фильтрующего брандмауэра отсеиваются недопустимые обращения к узлам внутренней сети, и запрещается передача из внутренней сети в Интернет для пакетов, определенных правилами фильтрации.

В целях получения более гибкой системы правила фильтрации пакетов составляются для каждого сетевого интерфейса, в них учитываются IP-адреса источника и получателя, номера портов TCP и UDP, флаги TCP-соединений и ICMP-сообщений. Причем правила для входящих и исходящих пакетов различаются. Это значит, что при настройке фильтрующего брандмауэра правила для конкретного сетевого интерфейса представляются как отдельные правила для входящей и исходящей информации, поскольку входящие и исходящие пакеты обрабатываются брандмауэром независимо друг от друга. Списки правил, которые управляют фильтрацией сетевых пакетов, поступающих извне в локальную сеть и отправляемых из локальной сети в Интернет, принято называть цепочками (chains). Термин "цепочка" используется потому, что при проверке пакета правила применяются последовательно одно за другим, пока не обнаружится подходящее правило для сетевого пакета или список правил не будет исчерпан.

Описанный механизм фильтрующего брандмауэра достаточно эффективен, однако он не обеспечивает полной безопасности локальной сети.

Брандмауэр всего лишь один из элементов общей схемы защиты. Анализ заголовков сетевых пакетов – операция слишком низкого уровня, для того чтобы реально выполнять аутентификацию и контролировать доступ. В процессе фильтрации пакетов практически невозможно распознать отправителя сообщения и проанализировать смысл передаваемой информации. Из всего набора данных, пригодных для аутентификации, на рассматриваемом уровне доступен только IP-адрес отправителя, однако этот адрес очень легко подделать, на чем и базируется множество способов сетевых атак. Несмотря на то, что средства фильтрации пакетов позволяют эффективно контролировать обращение к портам, использование протоколов обмена и содержимое пакетов, проверку данных необходимо продолжить на более высоком уровне.

Политика организации брандмауэра

При построении брандмауэров используются два основных подхода:

1. запрещается прохождение всех пакетов, пропускаются лишь те, которые удовлетворяют явно определенным правилам;

2. разрешается прохождение всех пакетов, за исключением пакетов, удовлетворяющих определенным правилам.

Другими словами, запрещено все, что не разрешено, и разрешено все, что не запрещено.

С практической точки зрения лучше использовать подход, при котором поступающий пакет по умолчанию отвергается (запрещено все, что не разрешено). В этом случае организация безопасности сети достигается достаточно просто, но с другой стороны, приходится предусматривать возможность обращения к каждой сетевой службе и использование каждого конкретного протокола. Это означает, что администратор сети, занимающийся настройкой брандмауэра, должен точно знать, какие протоколы применяются в его локальной сети. При использовании подхода, предусматривающего запрет по умолчанию, приходится предпринимать специальные меры всякий раз, когда

необходимо разрешить доступ к какому-то ресурсу, однако эта модель с нашей точки зрения более надежна, чем противоположный вариант.

Политика разрешения по умолчанию позволяет добиться функционирования системы малыми усилиями, но при этом необходимо предусмотреть каждый конкретный случай, при котором требуется запретить доступ.

Может случиться так, что необходимость внесения запретов станет ясна лишь тогда, когда в результате несанкционированного доступа сети будет нанесен значительный ущерб.

В обоих случаях для конфигурации брандмауэра используются цепочки правил. Каждая цепочка представляет собой набор правил, заданных явным образом, и политику по умолчанию.

Пакет проверяется на соответствие каждому из правил, а правила выбираются из списка последовательно до тех пор, пока не будет обнаружено соответствие сетевого пакета одному из них. Если пакет не удовлетворяет ни одному из заданных правил, с сетевым пакетом производятся действия, определенные политикой по умолчанию.

В процессе работы брандмауэр может пропустить сетевой пакет (ACCEPT), запретить прохождение сетевого пакета (DENY) либо отказать сетевому пакету в прохождении, т. е. отклонить его (REJECT).

При отклонении сетевого пакета (REJECT) сам пакет удаляется, а его отправителю возвращается ICMP-сообщение об ошибке.

При запрете прохождения сетевого пакета (DENY) сам пакет удаляется, но отправитель не оповещается об удалении сетевого пакета.

В большинстве случаев запрет сетевого пакета считается лучшим решением, чем отказ в прохождении сетевого пакета. Во-первых, отправка сообщения об ошибке увеличивает сетевой трафик, а во-вторых, сообщения об ошибке могут быть использованы для организации атаки с целью вывода из строя сервера.

Помимо этого, любое ответное действие на "неправильные" пакеты предоставляет взломщику дополнительную информацию о конфигурации системы.

2.2. Работа с утилитой UFW (Uncomplicated Firewall)

UFW (Uncomplicated Firewall) - является самым простым и довольно популярным инструментарием командной строки для настройки и управления брандмауэром в дистрибутивах Ubuntu и Debian. Правильно функционирующий брандмауэр является наиболее важной частью полной безопасности системы Linux. UFW позволяет сделать базовые настройки, для более сложных настроек рекомендуется использовать iptables.

Проверить текущий статус и вывести все текущие правила можно с помощью следующей команды:

sudo ufw status verbose

Например, в выключенном состоянии вы увидите следующее сообщение:

Status: inactive

Включить firewall можно с помощью следующей команды:

sudo ufw enable

Политики по умолчанию

По умолчанию брандмауэр UFW отклоняет все входящие соединения и разрешает только исходящие подключения к серверу. Это означает, что никто не может получить доступ к вашему серверу, если только вы специально не открываете порт, а все запущенные службы или приложения на вашем сервере могут иметь доступ к внешней сети.

Политики безопасности по умолчанию находятся в файле /etc/default/ufw и могут быть изменены с помощью следующей команды:

sudo ufw default deny incoming

sudo ufw default allow outgoing

Первое правило запрещает все входящие подключения, второе разрешает исходящие.

Работа с портами

Для открытия портов используется ключевое слово allow.

С помощью следующей команды можно открыть порт для входящих подключений:

sudo ufw allow <порт>/<протокол>

Например:

sudo ufw allow 1234/tcp

Также можно открывать порты по именам конкретных сервисов, например:

sudo ufw allow http

Примечание: если сервер использует порт не по умолчанию, то данное правило использовать нельзя.

ufw позволяет открывать или закрывать промежуток портов:

sudo ufw allow <портN>:<портM>/<протокол>

Например:

sudo ufw allow 5000:5003/udp

Для закрытия портов используйте ключевое слово deny. Синтаксис ufw остается прежним, только allow заменяется на deny. Например, чтобы закрыть порт используется следующая команда:

sudo ufw deny <порт>/<протокол>

Например:
sudo ufw deny 1234/tcp

Работа с IP-адресами

Чтобы разрешить соединение ко всем портам сервера с конкретного IP-адреса, используйте следующую команду:

sudo ufw allow from <IP-адрес>

К примеру:
sudo ufw allow from 111.111.111.111

Также можно разрешить подключаться к конкретному порту с определенного IP-адреса:

sudo ufw allow from <IP-адрес> to any port <порт>

Пример:
sudo ufw allow from 111.111.111.111 to any port 22

Для запрета подключения используйте ключевое слово deny:

sudo ufw deny from <IP-адрес>

Пример:
sudo ufw deny from 111.111.111.111

Работа с сетевым интерфейсом

С помощью ufw можно настроить подключение к конкретному порту определенного интерфейса:

sudo ufw allow in on <имя интерфейса> to any port <порт>

Например:

sudo ufw allow in on eth2 to any port 22

Примечание: имена всех интерфейсов сервера можно просмотреть с помощью команды ifconfig -a.

Удаление правил

Для удаления правил выведете нумерованный список текущих правил:

sudo ufw status numbered

Удалите правила под нужным номером:

sudo ufw delete <номер_правила>

Пример:

sudo ufw delete 1

Также можно удалить правило с помощью ключевого слова delete, например:

sudo ufw delete allow 443

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1) Для начала необходимо установить веб-сервер. В данной работе будет использоваться веб-сервер Apache

sudo apt install apache2 -y

2) Проверить, что всё установилось верно – необходимо ввести в браузере IP-адрес сервера, после чего откроется стандартная страница Apache (рисунок 1).

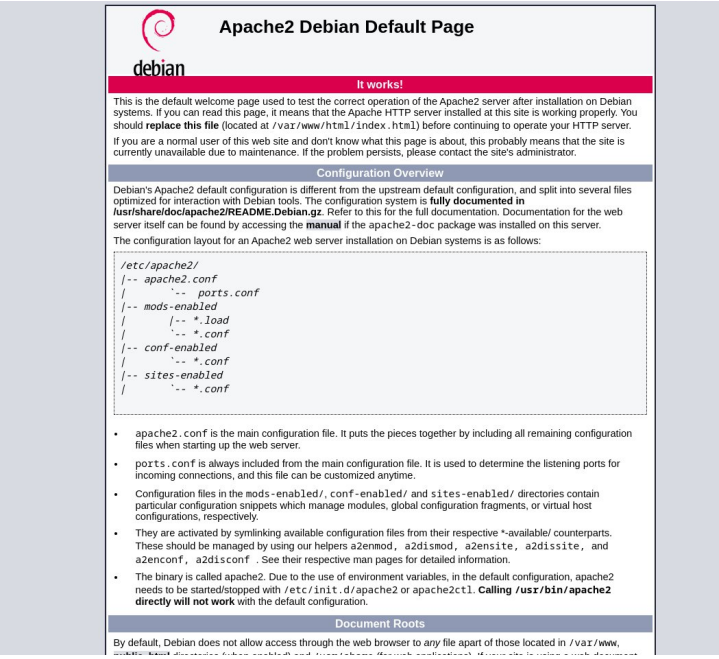

Рисунок 1 – Стандартная страница Apache

IP-адрес можно узнать выполнив следующую команду (рисунок 2):

ip -br a

Рисунок 2 – Локальный IP-адрес машины

3) Разместить на сервере содержимое сайта mysite.com, для этого создать необходимые директории и сделать их владельцем пользователя, который будет работать с сайтом:

sudo mkdir /var/www/mysite.com

sudo chown -R $USER:$USER /var/www/mysite.com

sudo chmod –R 755 /var/www/mysite.com

4) Добавить на сайт html страницу, для этого создать файл index.html:
touch /var/www/mysite.com/index.html

5) Необходимо создать файл виртуального хоста и заполнить его:

touch /etc/apache2/sites-available/mysite.com.conf

В этот файл необходимо поместить следующее:

```
<VirtualHost *:80>
        ServerAdmin admin@mysite.com
        ServerName mysite.com
        ServerAlias www.mysite.com
        DocumentRoot /var/www/mysite.com
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

6) Включить сайт , для этого сделать символьную ссылку на файл конфигурации в каталоге sites-enabled. Это можно сделать при помощи специальной утилиты Apache:
sudo a2ensite mysite.com

7) Отключить стандартный сайт Apache, определённый в файле 000-default.conf, для этого необходимо выполнить следующую команду:
sudo a2dissite 000-default.conf

8) Перезапустить веб-сервер, команда, которая позволяет это сделать:
sudo systemctl restart apache2

После этого, если перейти в браузере на IP-адрес сервера, то вместо стандартной страницы Apache будет отображаться созданная ранее страница index.html (рисунок 3).

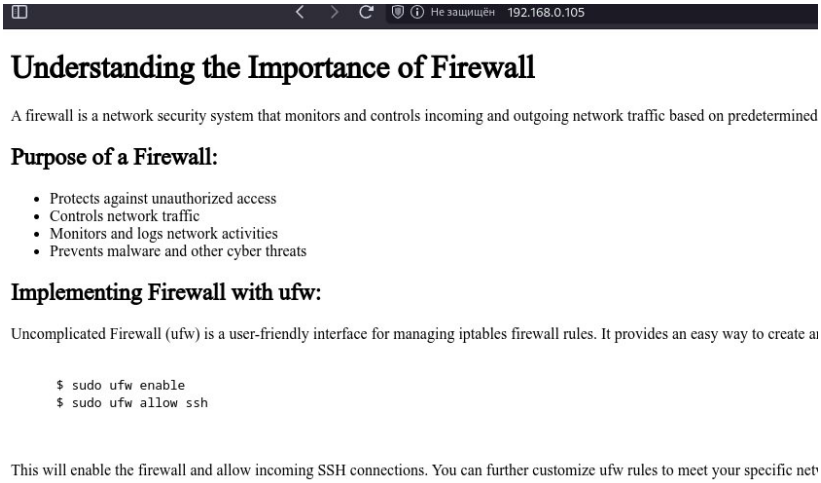

Рисунок 3 – Созданная html страница

9) Установить утилиту для работы с брандмауэром UFW (Uncomplicated Firewall):

sudo apt install ufw

Чтобы включить UFW необходимо выполнить следующую команду в терминале:

sudo ufw enable

10) Разрешить входящие соединения через порт, который использует веб-сервер (обычно 80 – для HTTP и 443 – для HTTPS), для этого добавить новое правило, выполнив следующую команду:

sudo ufw allow 'WWW'

А затем перезапустить утилиту:

sudo ufw reload

Теперь, при попытке открыть IP-адрес сервера с другого устройства в локальной сети, можно будет получить доступ к странице index.html (рисунок 4).

Рисунок 4 – Веб-сервер, открытый с устройства локальной сети

4. Контрольные вопросы

1. Что такое брандмауэр? Типы брандмауэров.

2. Политика разрешения и политики запрещения.

3. Поясните понятия: пропускание, запрещение и отклонение сетевого пакета

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ботте Т. Руководство администратора сети/ Т. Ботте, Т. Доусон, Г. Перди. – Кудиц-Образ, 2004.– 386с.

2. «UFW Community Help Wiki» (help.ubuntu.com/community/UFW) [Электронный ресурс]. — Режим доступа: https://help.ubuntu.com/community/UFW