ПРАКТИЧЕСКАЯ РАБОТА №2

# Дополнительная настройка хостов ОС Linux

**Цель работы:** получить практические навыки работы c дополнительными с инструментальными средствами настройки доступа к хосту в ОС Linux.

**Необходимо:**

* Установленная на компьютере среда виртуализации ORACLE Virtual Box
* Образы виртуальной машины Linux Cent OS 7 (выполнять работу можно в любой ОС Linux, но все описания будут даваться для CentOS 7).

**Краткие теоретические сведения:**

Linux сейчас является основной операционной системой для развертывания сервисов обработки данных. ОС Linux содержит необходимые средства для организации защищенного удаленного доступа и организации Интернет-шлюза.

NAT (Network Address Translation) – технология стека TCP\IP. Она позволяет модифицировать заголовки пересылаемых через NAT IP-пакетов и TCP\UDP сообщений.

NAT в общем случае представляет собой компьютер или аппаратный маршрутизатор, подключенный одним интерфейсом к внешней сети, а другими к внутренней. Оба интерфейса имеют IP адреса в каждой из сетей. Типичным применением NAT является обеспечение доступа из локальной сети с приватными IP-адресами к ресурсам внешней сети с IP-адресами интернет. При передаче запроса от локального клиента к внешнему ресурсу подменяется сокет отправителя: IP адрес меняется на внешний IP адрес NAT, а порт на свободный порт на внешнем интерфейсе NAT. Когда приходит ответ от внешнего ресурса, происходит обратная замена сокета и пакет передается в локальную сеть полкучателю. Так же с помощью NAT можно публиковать локальные сокеты на реальном IP адресе и реальном порту. Например для обеспечения доступа извне к Web серверу, расположенному в локальной сети. В этом случае на NAT делается статическое отображение внешнего сокета на внутренний.

Под межсетевым экраном или брандмауэром понимают фильтр IP пакетов предназначенный для формального ограничения соединений клиентов и серверов работающих «поверх» стека TCP\IP.

В основу работы классического firewall положен контроль формальных признаков. В общем случае фильтрация осуществляется по:

• IP адресам отправителя и получателя в заголовке IP пакета

• номерам портов приложения-получателя и приложения-отправителя

• инкапсулированным в IP протоколам транспортного (TCP, UDP) и сетевого уровней (ICMP).

Правила фильтрации формируются в виде списка. Все проходящие пакеты проверяются по списку последовательно, до первого срабатывания. Последующие правила к пакету не применяются.

Для управления шлюзом используются различные инструменты управления брандмауэром Linux, такие как iptables, nftables и firewalld.

В CentOS 7 используется firewalld. Для управления им служит утилита **firewall-cmd**.

Важно отметить, что для того чтобы Linux начал пересылать пакеты из интерфейса в интерфейс надо чтобы в параметре ядра net.ipv4.ip\_forward = 1. Установить его можно с помощью утилиты sysctl, или записью в конфигурационный файл в каталоге /proc.

В Linux для удаленного доступа к серверам используется протокол SSH (secure shell). Он создает шифрованное соединение между клиентом и сервером. Благодаря этой технологии может осуществляться удаленное управление компьютером.

Сервер ssh (openssh-server) устанавливается по умолчанию и выполняется службой sshd. Конфигурация сервера осуществляется в конфигурационном файле /etc/ssh/sshd\_config.

Для управления запуском и просмотра состояния сервиса используется системная утилита systemctl.

**Инструментальные средства:**

Утилиты: sysctl firewall-cmd systemctl useradd chmod ip ping su sudo usermod

Файлы: /etc/ssh/sshd\_config

Утилиты работы с текстом: echo, grep, sed

Редакторы: vi, nano

**Порядок выполнения работы:**

Далее описан порядок выполнения работы. Пункты работы, результаты которых прямо или косвенно используются в отчете, помечены знаком **(!)**.

**Часть 1. Проверка конфигурации.**

1. В работе используются виртуальные машины, сконфигурированные в предыдущей работе.
2. Запустите системы c7-1 и c7-2, авторизуйтесь с правами root.
3. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7-1.
4. Убедитесь, что на c7-2 в качестве шлюза по умолчанию задан адрес c7-1.

**Часть 2. Создание пользователей и настройка sshd.**

1. На хосте c7-2 создайте пользователя с именем FIOuser, где FIO – ваши инициалы. **(!)**.
2. Зайдите на вторую консоль под вашим пользователем.
3. По системным журналам определите, когда был создан пользователь и когда, он зашел в систему. **(!)**.
4. Настройте ssh сервер так, чтобы **(!)**.:
   1. Пользователю root нельзя было бы входить по ssh
   2. Количество попыток ввода неверного пароля = 2
   3. Время ожидания авторизации = 30 секундам.
5. После перезапуска выведите на консоль состояние сервиса sshd и его журнал средствами systemd **(!)**.
6. С машины с7-1 подключитесь к с7-2 по ssh, используя новую учетную запись.
7. На консоли c7-2 с помощью утилиты su войдите на консоль root.
8. Добавьте нового пользователя в группу wheel (группа для работы через sudo). **(!)**.
9. Выйдете из консоли root. От имени нового пользователя проверьте доступность по чтению файла с паролями пользователей без использования утилиты sudo и с ней.

**Часть 3. Настройка шлюза**

Цель этой части – настроить хост c7-1 как шлюз доступа к хосту c7-2. **(!)**.

1. Включите на хосте c7-1 пересылку пакетов через ядро с помощью утилиты sysctl. **(!)**
2. С помощью утилиты firewall-cmd настройте c7-1 так, чтобы:
   1. Запросы от c7-2 транслировались во внешнюю сеть
   2. На порту с номером 55022 внешнего сетевого интерфейса c7-1 был опубликован порт 22 на хосте с7-2.
3. Подключитесь к серверу c7-2 с вашей реальной операционной системы (используйте публикацию портов в NAT в VirtualBox или Сетевой Мост).
4. С помощью команды who выведите список пользователей на хосте c7-2. **(!)**

**Часть 4. Управление процессами**

1. На машине с7-2 от имени созданного пользователя запустите редактор vi.
2. На другой консоли, работая от пользователя root определите PID и PPID процесса vi. **(!)**
3. Завершите процесс используя сигнал безусловного завершения (сигнал KILL). **(!)**
4. Убедитесь в завершении процесса.

**Часть 5. Передача файлов**

1. Используя SSH передайте на машину c7-2 любой файл. Это можно сделать с помощью утилиты scp на Linux и утилиты pscp из комплекта утилиты Putty на Windows **(!).**

**Содержание отчета**

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы и задания.

Артефакты:

1. Текст команд и консольные выводы из Части 2 п.1,3,5,8
2. Измененные параметры файла конфигурации sshd из Части 2. п. 4.
3. Текст команд и консольные выводы из Части 3 п.1,4
4. Текст команд и консольные выводы из Части 4 п.2,3
5. Текст команд и консольные выводы из Части 5 п.1

Вопросы и задания:

1. Опишите, как вы проверили доступность машин в части 1.
2. Напишите конвейер команд, или команду или скрипт, позволяющий создать пользователя, сразу указав его пароль.
3. Поясните результаты выполнения п.9 Части 2.
4. В части 4 вы завершили процесс сигналом KILL. Почему это плохой способ завершения процесса?

Дополнительные материалы по теме курса публикуются на Telegram-канале ITSMDao (t.me/itsmdao). Обсуждать работу и задавать вопросы можно в чате ITSMDaoChat (t.me/itsmdaochat).