**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет прикладной информатики**

**Дисциплина:**

«Введение в Linux»

**ПРАКТИЧЕСКАЯ РАБОТА №4**

«Элементы безопасности в Linux»

**Выполнил:**

Мануковская Д. М.

Сакулин И. М.

Сафронов И. С.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверила:**

Береснев А. Д., старший преподаватель

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Содержание

[Содержание 2](#_Toc184827463)

[Постановка задачи 3](#_Toc184827464)

[Артефакты выполнения 4](#_Toc184827465)

[Ответы на вопросы 10](#_Toc184827466)

[Рефлексия 14](#_Toc184827467)

[Список использованных источников 15](#_Toc184827468)

Постановка задачи

**Цель работы** – получить практические навыки работы с сетевой подсистемой в Linux, научиться настраивать сетевые интерфейсы, NAT и настраивать ssh.

Применяемое в ходе выполнения практической работы ПО:

Утилиты: sysctl systemctl ip useradd ss iptables iptables-save iptables-restore ls

adduser passwd chmod chown who ssh-keygen scp sodo visudo.

Файлы: /etc/ssh/sshd\_config.

Утилиты работы с текстом: echo, grep, sed.

Редакторы: vi, nano.

Артефакты выполнения

**1.1 Файлы interfaces с обоих хостов.**

Текст файлов interfaces с машин с7-1 и с7-2 предоставлены на рисунках 1 и 2.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 – Файл interfaces с c7-1

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 2 – Файл interfaces с c7-2

**1.2 Консольный вывод из Части 2, п.3**

На рисунке 3 представлен консольный вывод команд, использовавшихся для подтверждения работы сервиса.

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

Автоматически созданное описание

Рисунок 3 – Консольный вывод из Части 2, п.3

**1.3 Консольный вывод из Части 3, п 5,6,8**

Консольные выводы команд ss, who, scp на рисунке 4.

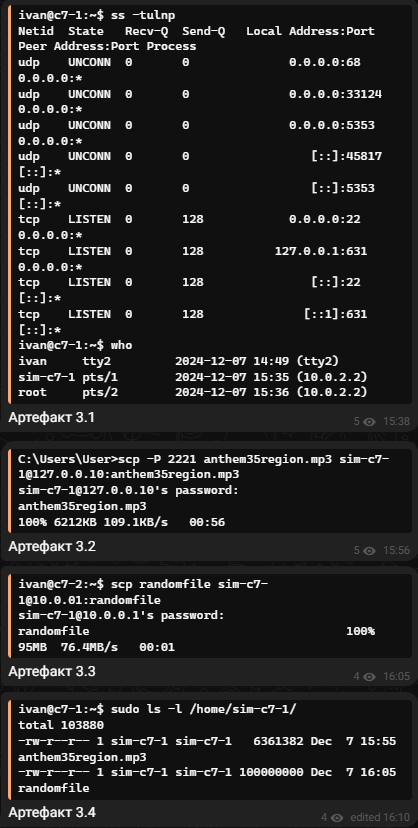


Рисунок 4 – Консольный вывод из Части 3, п 5,6,8

**1.4 Консольный вывод команды из части 4 п.8**

Вывод правил iptables представлен на рисунке 5.

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 5 – Консольный вывод команды из части 4 п.8

**1.5 Скрипт из Части 5, п.1**

На рисунке 6 код скрипта из части 5 п.1.

Изображение выглядит как текст, снимок экрана, Шрифт, меню

Автоматически созданное описание

Рисунок 6 – Скрипт из Части 5, п.1

**1.6 Консольный вывод из Части 5, п.8**

На рисунке 7 консольный вывод прав на файлы, каталоги из части 5.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 7 – Консольный вывод из Части 5, п.8

**1.7 Команды из части 6 п.1 и п. 5.**

Команды для создания пары ключей и копирования файла скрипта на реальный хост по ключу показаны на рисунке 8.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 8 – Команда из части 6 п.1 и п. 5.

**1.8 Измененные параметры конфигурационного файла из Части 6 п.3**

На рисунке 9 отредактированная конфигурация sshd.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

Рисунок 9 – Измененные параметры конфигурационного файла из Части 6 п.3

**1.9 Измененные параметры конфигурационного файла из части 7 п.3**

На рисунке 9 параметры измененного конфигурационного файла.



Рисунок 10 – Измененные параметры конфигурационного файла из части 7 п.3

**1.10 Консольный вывод из части 8 п.1 и п.2**

На рисунке 11 консольный вывод информации о входах пользователей за последний месяц из части 8.

Изображение выглядит как текст, снимок экрана, меню, дизайн

Автоматически созданное описание

Рисунок 11 – Консольный вывод из части 8 п.1

На рисунке 12 консольный вывод информации командой о пользователе из части 8.



Рисунок 12 – Консольный вывод из части 8 п.2

Ответы на вопросы

**2.1 ВОПРОС 1**

Эта команда iptables настраивает трансляцию сетевых адресов (NAT) для перенаправления входящего трафика на порт 55022 на внутренний IP-адрес. Разберем её по частям:

1) iptables: Это сама утилита iptables, которая используется для управления правилами брандмауэра и NAT в Linux.

2) -t nat: Этот параметр указывает iptables работать с таблицей nat. Таблица nat отвечает за правила трансляции сетевых адресов (NAT), которые изменяют IP-адреса и порты пакетов. Другие таблицы iptables (filter, mangle, raw) служат для разных целей.

3) -A PREROUTING: Это указывает iptables добавить новое правило (-A) в цепочку (PREROUTING). Цепочка PREROUTING обрабатывает пакеты до того, как маршрутизатор решит, куда их направить. Это важно для NAT, так как нужно изменить адрес до того, как маршрутизация определит, куда передать пакет.

4) -i ИМЯ-СЕТЕВОГО-ИНТЕРФЕЙСА-NAT: Этот параметр указывает интерфейс, на котором iptables будет прослушивать входящий трафик. ИМЯ-СЕТЕВОГО-ИНТЕРФЕЙСА-NAT Замените на фактическое имя сетевого интерфейса (например, eth0, wlan0), который подключен к внешней сети и на который поступает трафик, который нужно перенаправить.

5) -p tcp: Этот параметр задает протокол, к которому применяется правило. tcp означает, что правило относится только к трафику TCP.

6) -dport 55022: Этот параметр указывает порт назначения (destination port) входящего трафика. Правило будет срабатывать только для пакетов, направленных на порт 55022 на внешнем интерфейсе.

7) -j DNAT: Этот параметр указывает действие (-j), которое необходимо выполнить при совпадении условий. DNAT означает NAT назначения — изменение адреса назначения пакета.

8) --to-destination 10.0.0.2:22: Этот параметр указывает новый адрес и порт назначения. 10.0.0.2 — это внутренний IP-адрес, на который будет перенаправляться трафик, а 22 — это порт на этом внутреннем адресе (обычно порт SSH).

**2.2 ВОПРОС 2**

Пароль, вводимый при создании ssh ключей, нужен для шифрования ключа. Это дополнительная защита, при подключении с ключом будет спрашиваться не пароль пользователя, а самого ключа.

**2.3 ВОПРОС 3**

1) Проверка подлинности сервера: SSH использует криптографию с открытым ключом для аутентификации. Сервер имеет пару ключей: закрытый (хранится в секрете на сервере) и открытый (доступен клиенту). Отпечаток ключа (хэш) — это криптографическая «подпись» открытого ключа. При первом подключении к серверу ваш SSH-клиент сравнивает этот отпечаток с тем, который он ожидает получить от настоящего сервера. Если отпечатки совпадают, это подтверждает, что вы подключаетесь к тому серверу, к которому намеревались подключиться, а не к злоумышленнику, который подделал сервер под видом настоящего.

2) Защита от атак «человек посередине»: если злоумышленник перехватывает соединение между вашим компьютером и сервером (атака «человек посередине»), он может подменить свой собственный сервер. Предлагаемый отпечаток позволит вам обнаружить такую атаку, поскольку отпечаток поддельного сервера будет отличаться от ожидаемого.

3) Предотвращение будущих предупреждений: после того как вы приняли отпечаток ключа, он сохраняется в вашем списке известных хостов. При последующих подключениях к этому серверу проверка отпечатка будет выполняться автоматически, и вам не будет выводиться запрос на подтверждение.

**2.4 ВОПРОС 4**

Подключенные ssh соединения можно посмотреть через команду: ss -a | grep ssh . Ключ -а нужен для вывода всех сокетов (открытых соединений).

Для вывода открытых ssh соединений сервера можно использовать команду: ps auxwww | grep sshd: | grep -v grep . Значение аргументов:

a – показать все процессы

u – столбцы с информацией о пользователе

x – показать процессы не связанные с терминалов

w – широкий вывод, при повторе выключает ограничение ширины

**2.5 ВОПРОС 5**

Понять, что у пользователей одинаковый пароль из /etc/shadow нельзя. При создании пароля генерируется случайный текст (соль) и дописывается к введенному паролю. Далее происходит шифрование полученной строки. Т.к соль всегда будет различной, то и соленый хэши – зашифрованные пароли будут разные.

**2.6 ВОПРОС 6**

Таблица представлена на рисунке 13.

Изображение выглядит как текст, снимок экрана, документ, Шрифт

Автоматически созданное описание

Рисунок 13 – Таблица атрибутов

**2.7 ВОПРОС 7**

Команда setfacl позволяет управлять расширенными списками контроля доступа (ACL) в Linux. Для предоставления конкретному пользователю всех прав на файл, не меняя владельца и группы, можно использовать следующую команду:

setfacl -m u:имя\_пользователя:rwx файл

setfacl: Утилита для управления ACL.

-m: Опция для добавления новой записи в ACL.

u:имя\_пользователя: указывает пользователя, которому нужно предоставить права. Замените имя\_пользователя на реальное имя пользователя.

rwx: Права доступа: чтение (r), запись (w), выполнение (x).

файл: Путь к файлу, для которого устанавливаются права.

Пример:

Чтобы дать пользователю vboxuser все права на файл /home/user/my\_file, нужно выполнить команду:

sudo setfacl -m u: vboxuser:rwx /home/user/my\_file

Рефлексия

Цель работы была достигнута. В ходе работы мы получили практические навыки работы с сетевой подсистемой в Linux, научились настраивать сетевые интерфейсы, NAT и настраивать ssh.

Список использованных источников

1. Losst // Режим доступа: <https://losst.pro/>

(даты обращения: 10.12.2024)