

Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут»

# Лабораторна робота №7

***з дисципліни «Комп’ютерні мережі»***

**«Пакетні фільтри»**

Виконав студент групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ 2024**

***Мета роботи***

Поглиблене самостійне вивчення спеціальних питань, присвячених організації та конфігуруванню брандмауера, що використовує iptables.

***План виконання лабораторної роботи***

1. Ознайомитися та засвоїти теоретичні відомості викладені в навчально-методичному посібнику до лабораторної роботи.

2. Виконати завдання до лабораторної роботи. Скласти звіт.

***Завдання***

1. Дозволити приймати пакети лише з хоста scs.kpi.ua. Виконайте перевірку дії встановлених правил.
2. Заборонити з’єднання з вашою машиною з комп’ютерів в локальній мережі.
3. Відключити відклик на ICMP запити на вашій машині. Виконайте перевірку дії встановлених правил.
4. Закрити всі порти, крім SMTP. Виконайте перевірку дії встановлених правил.
5. Створити ланцюжок користувача spammsg. В цьому ланцюжку записати правило, за яким усі повідомлення від джерела спаму будуть знищуватися. Виконати перехід з ланцюжка INPUT на ланцюжок spammsg.
6. Показати викладачу.

***Теоретичні відомості***

**Iptables** — це потужна утиліта командного рядка для налаштування і управління таблицями правил брандмауера у системах на базі ядра Linux. Вона забезпечує контроль над потоком мережевих пакетів, що проходять через систему, дозволяючи створювати складні правила для їх фільтрації.

**Основні поняття:**

1. **Таблиці:**
   * Iptables працює з кількома таблицями, кожна з яких має специфічне призначення:
     + **Filter**: за замовчуванням використовується для фільтрації пакетів (INPUT, OUTPUT, FORWARD).
     + **Nat**: використовується для зміни адрес або портів (SNAT, DNAT, MASQUERADE).
     + **Mangle**: дозволяє модифікувати заголовки пакетів (TTL, TOS).
     + **Raw**: виключає певні пакети з обробки відстеження станів.
     + **Security**: застосовується для встановлення політик SELinux.
2. **Ланцюжки (Chains):**
   * Кожна таблиця містить набір вбудованих ланцюжків:
     + **INPUT**: обробка вхідного трафіку.
     + **OUTPUT**: обробка вихідного трафіку.
     + **FORWARD**: обробка трафіку, що пересилається між інтерфейсами.
3. **Правила (Rules):**
   * Кожне правило визначає умови, за яких пакет обробляється, і дію (target), яка виконується:
     + **ACCEPT**: дозволити пакет.
     + **DROP**: відхилити пакет без відповіді.
     + **REJECT**: відхилити пакет з повідомленням.
     + **LOG**: записати інформацію про пакет у журнал.
     + **SNAT/DNAT**: змінити IP-адресу або порт.
4. **Модулі match і target:**
   * **match**: визначає критерії (IP-адреса, порт, протокол, розмір пакета, стан з'єднання).
   * **target**: вказує, що робити з пакетом (ACCEPT, DROP, DNAT тощо).

**Практичні можливості Iptables:**

1. **Фільтрація пакетів:**
   * Обмеження доступу до певних портів, IP-адрес або протоколів.
   * Приклад: iptables -A INPUT -s 192.168.1.1 -j DROP (блокувати доступ з IP 192.168.1.1).
2. **Блокування ICMP-запитів:**
   * Використовується для запобігання пінг-запитів:  
     iptables -A INPUT -p icmp --icmp-type echo-request -j DROP.
3. **Налаштування NAT:**
   * SNAT: зміна вихідної IP-адреси.  
     iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.1.100.
   * DNAT: перенаправлення вхідних запитів.  
     iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.1.101.
4. **Журналювання пакетів:**
   * Запис інформації про заблоковані або підозрілі пакети:  
     iptables -A INPUT -j LOG --log-prefix "Blocked Packet: ".
5. **Створення користувацьких ланцюжків:**
   * Наприклад, для обробки спам-пакетів:

iptables -N spammsg

iptables -A spammsg -s 192.168.1.2 -j DROP

iptables -A INPUT -j spammsg

1. **Використання станів з'єднань:**
   * Дозвіл лише встановлених і пов'язаних з'єднань:  
     iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT.
2. **Закриття портів:**
   * Всі порти, окрім необхідних (наприклад, SMTP):

iptables -P INPUT DROP

iptables -A INPUT -p tcp --dport 25 -j ACCEPT

***Хід роботи***

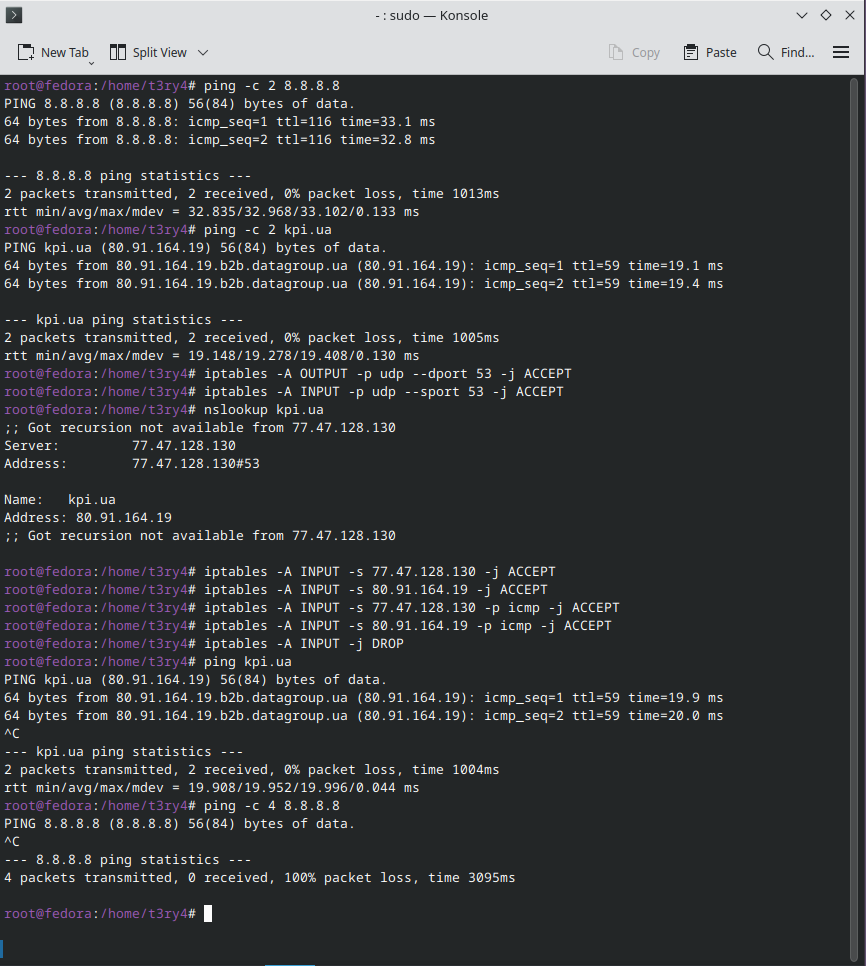
******

Рис. 1 – Перевірка прийому пакетів лише з хоста kpi.ua.

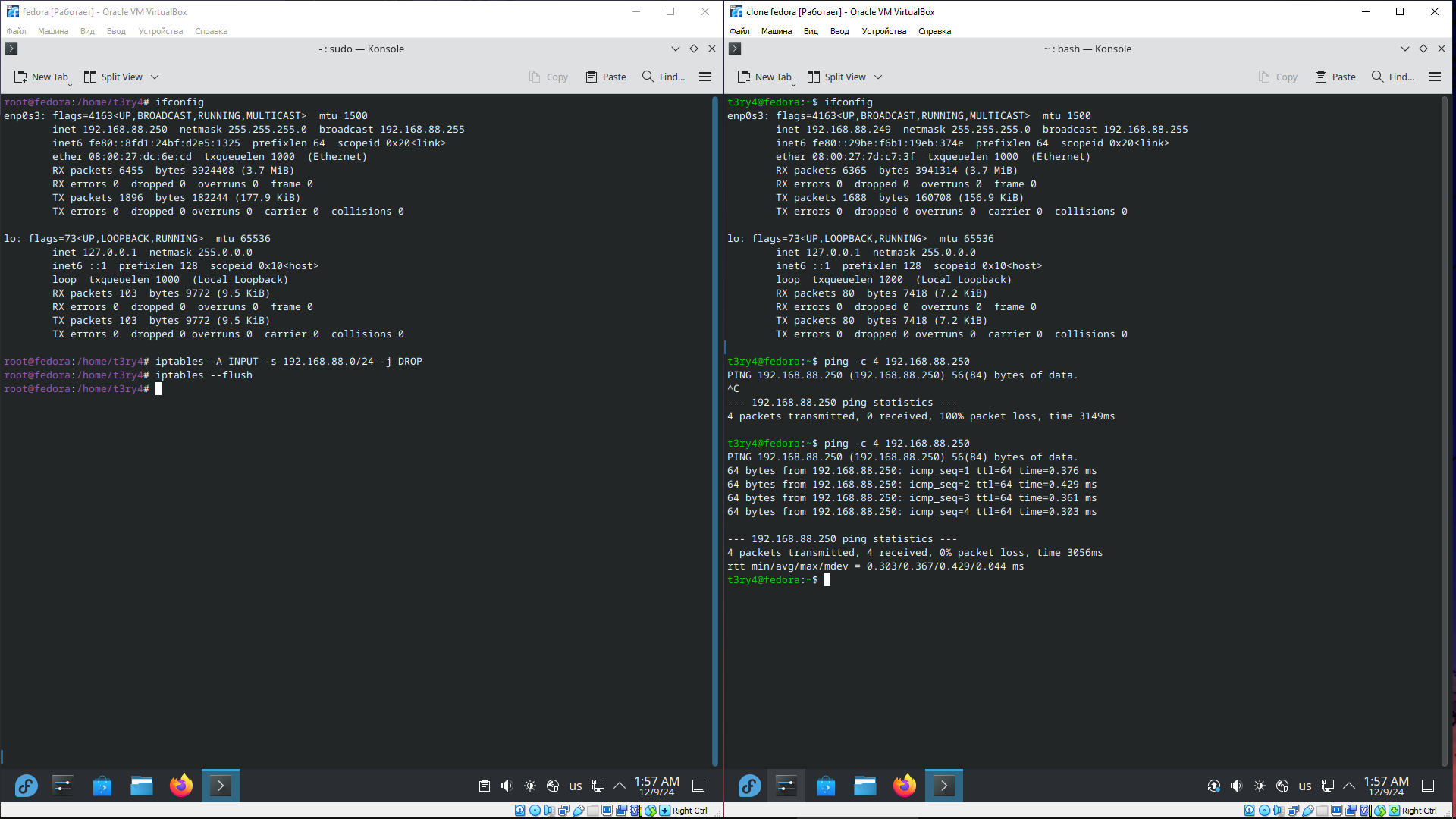


Рис. 2 – Заборона з’єднання з комп’ютерів локальної мережі.

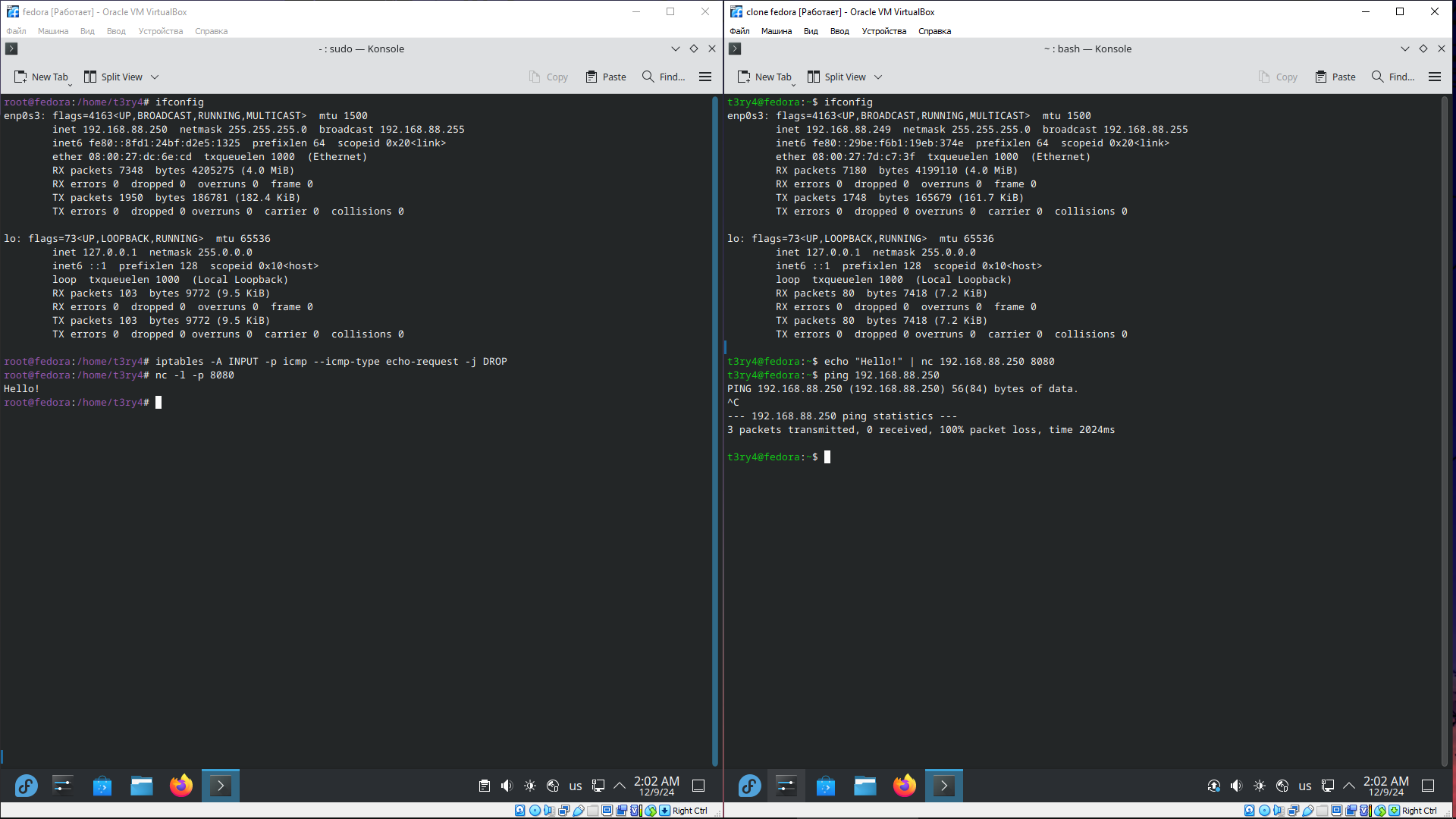


Рис. 3 – Відключення відповіді на ICMP-запити.

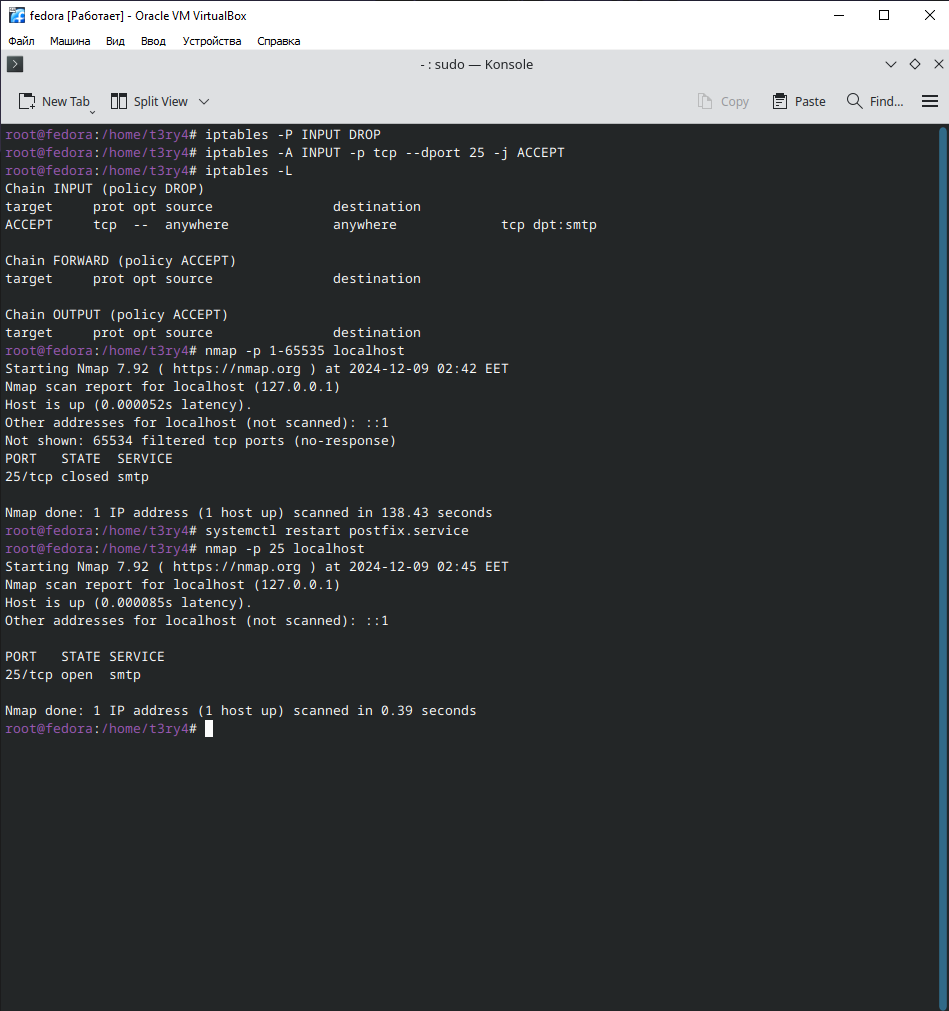


Рис. 4 – Закриття всіх портів, окрім SMTP.

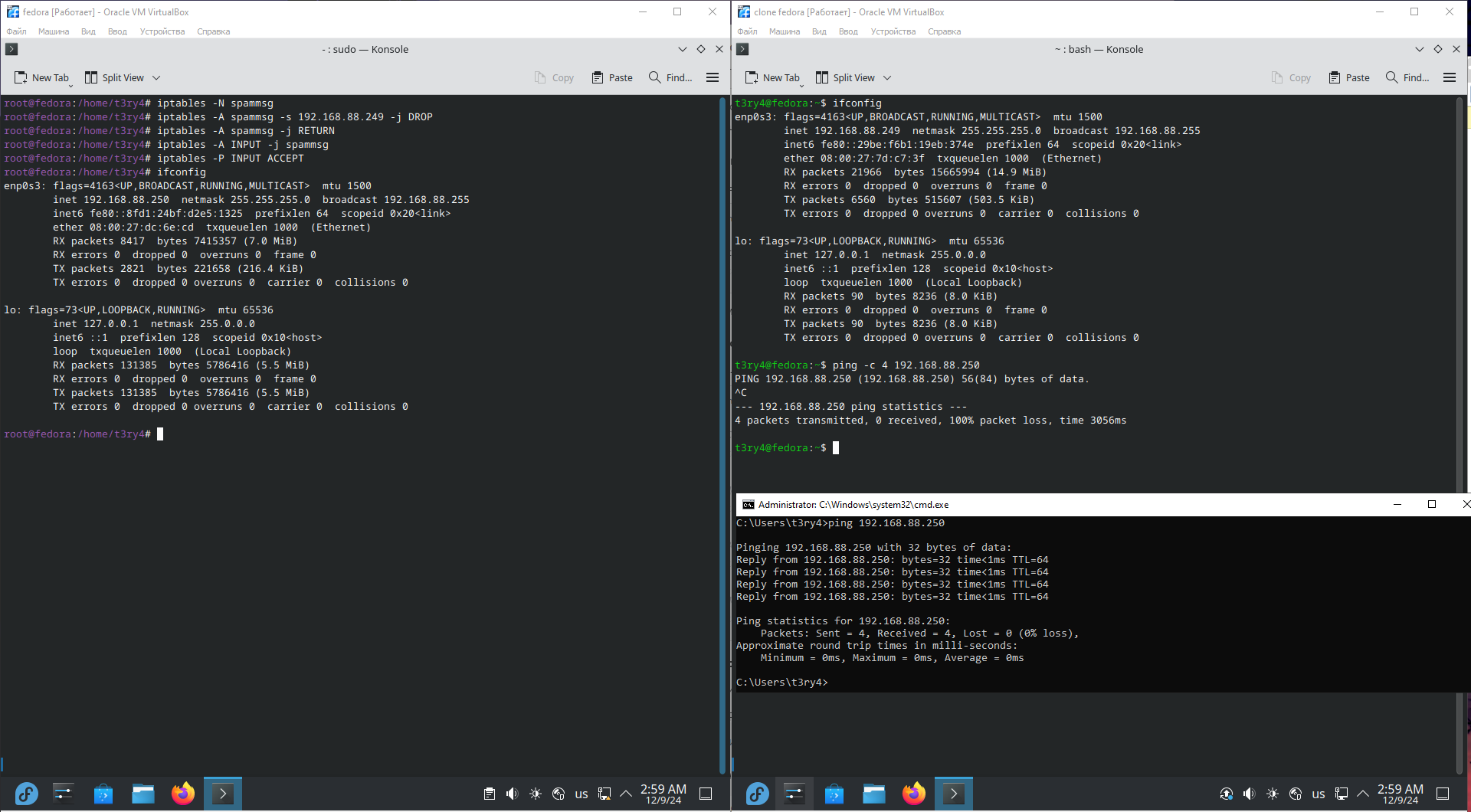


Рис. 5 – Створення ланцюжка spammsg для блокування джерел спаму.

***Висновок***

У ході виконання лабораторної роботи ми ознайомилися з основними можливостями утиліти **iptables** для управління правилами фільтрації пакетів у системах на базі Linux. Були налаштовані різні сценарії обмеження та контролю мережевого трафіку, зокрема:

* Дозволено прийом пакетів лише від певного хоста.
* Заборонено з’єднання з машиною з локальної мережі.
* Відключено ICMP-відгуки, що підвищує безпеку системи.
* Заблоковано всі порти, крім одного, необхідного для роботи (SMTP).
* Реалізовано створення користувацького ланцюжка для обробки небажаних джерел трафіку.

Ця робота допомогла закріпити знання щодо налаштування брандмауера та базових принципів мережевої безпеки. Отримані навички мають практичне застосування для забезпечення захищеності системи від небажаних з’єднань та атак.