

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: _____

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 мережових 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
```

6. Використання станів з'єднань:

- Дозвіл лише встановлених і пов'язаних з'єднань:
`iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`.

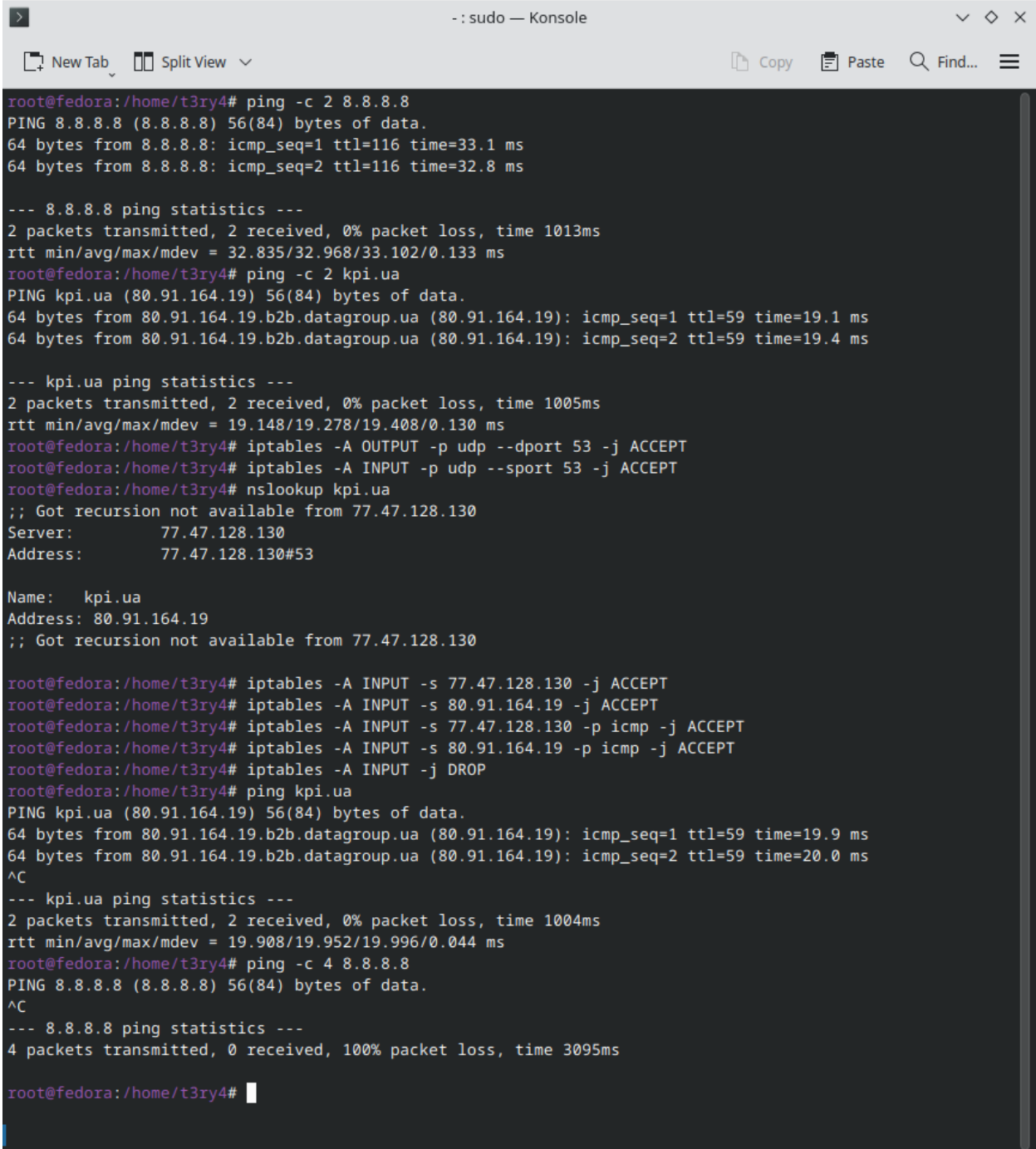
7. Закриття портів:

- Всі порти, окрім необхідних (наприклад, SMTP):

```
iptables -P INPUT DROP
```

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

Хід роботи

A screenshot of a terminal window titled ': sudo — Konsole'. The terminal shows a series of commands and their outputs. The user is in the directory /home/t3ry4. The commands include: 1. Ping test to 8.8.8.8 with 2 packets, showing successful results with TTL=116. 2. Ping test to kpi.ua (80.91.164.19) with 2 packets, showing successful results with TTL=59. 3. Firewall configuration using iptables to allow UDP traffic on port 53 from both 8.8.8.8 and kpi.ua. 4. A nslookup for kpi.ua showing its IP address as 80.91.164.19. 5. Firewall configuration using iptables to allow ICMP traffic from both 8.8.8.8 and kpi.ua. 6. A final ping test to 8.8.8.8 with 4 packets, which fails with 100% packet loss. The terminal output is as follows:

```
root@fedora:/home/t3ry4# ping -c 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=33.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=32.8 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 32.835/32.968/33.102/0.133 ms
root@fedora:/home/t3ry4# ping -c 2 kpi.ua
PING kpi.ua (80.91.164.19) 56(84) bytes of data.
64 bytes from 80.91.164.19.b2b.datagroup.ua (80.91.164.19): icmp_seq=1 ttl=59 time=19.1 ms
64 bytes from 80.91.164.19.b2b.datagroup.ua (80.91.164.19): icmp_seq=2 ttl=59 time=19.4 ms

--- kpi.ua ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 19.148/19.278/19.408/0.130 ms
root@fedora:/home/t3ry4# iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
root@fedora:/home/t3ry4# iptables -A INPUT -p udp --sport 53 -j ACCEPT
root@fedora:/home/t3ry4# nslookup kpi.ua
;; Got recursion not available from 77.47.128.130
Server:          77.47.128.130
Address:         77.47.128.130#53

Name:   kpi.ua
Address: 80.91.164.19
;; Got recursion not available from 77.47.128.130

root@fedora:/home/t3ry4# iptables -A INPUT -s 77.47.128.130 -j ACCEPT
root@fedora:/home/t3ry4# iptables -A INPUT -s 80.91.164.19 -j ACCEPT
root@fedora:/home/t3ry4# iptables -A INPUT -s 77.47.128.130 -p icmp -j ACCEPT
root@fedora:/home/t3ry4# iptables -A INPUT -s 80.91.164.19 -p icmp -j ACCEPT
root@fedora:/home/t3ry4# iptables -A INPUT -j DROP
root@fedora:/home/t3ry4# ping kpi.ua
PING kpi.ua (80.91.164.19) 56(84) bytes of data.
64 bytes from 80.91.164.19.b2b.datagroup.ua (80.91.164.19): icmp_seq=1 ttl=59 time=19.9 ms
64 bytes from 80.91.164.19.b2b.datagroup.ua (80.91.164.19): icmp_seq=2 ttl=59 time=20.0 ms
^C
--- kpi.ua ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 19.908/19.952/19.996/0.044 ms
root@fedora:/home/t3ry4# ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3095ms

root@fedora:/home/t3ry4#
```

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

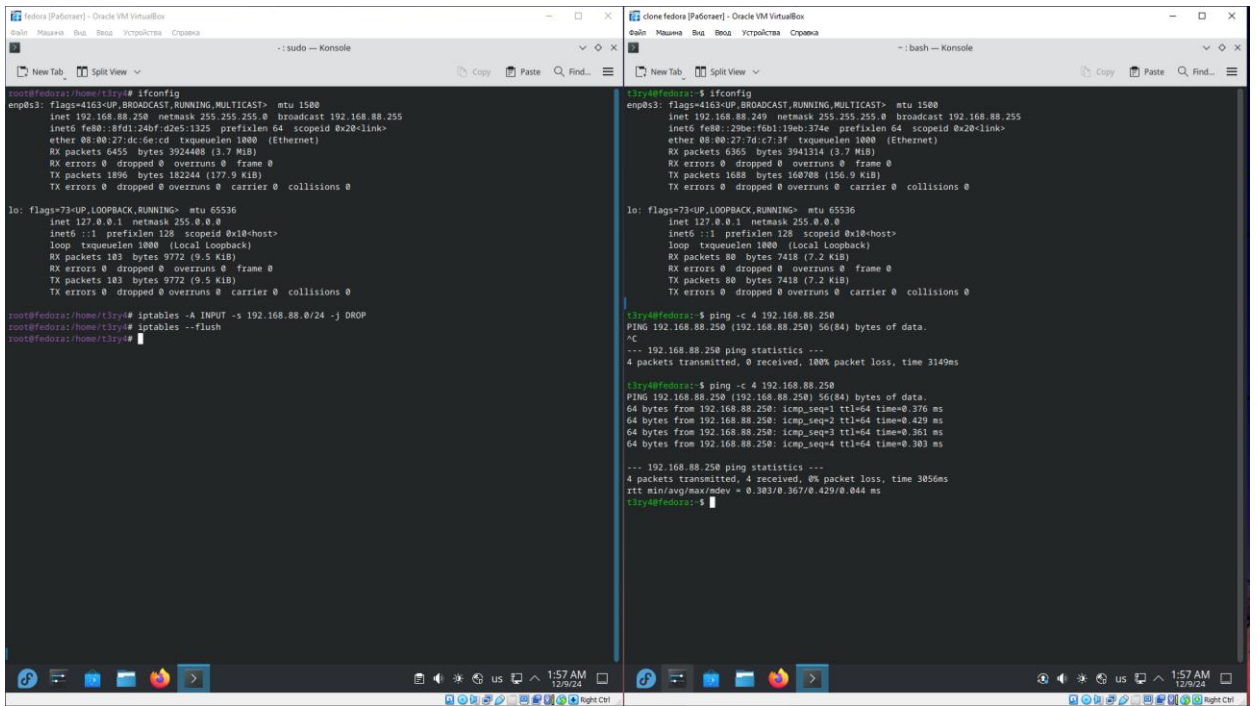


Рис. 2 – Заборона з'єднання з комп'ютерів локальної мережі.

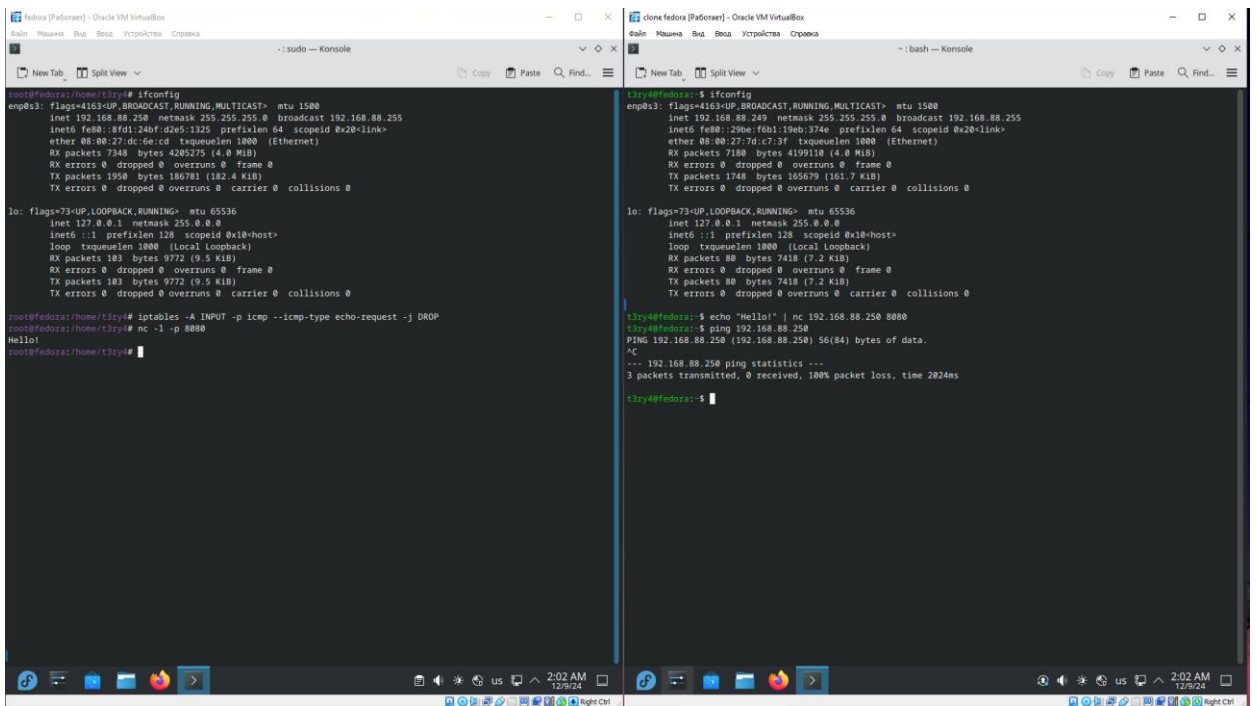
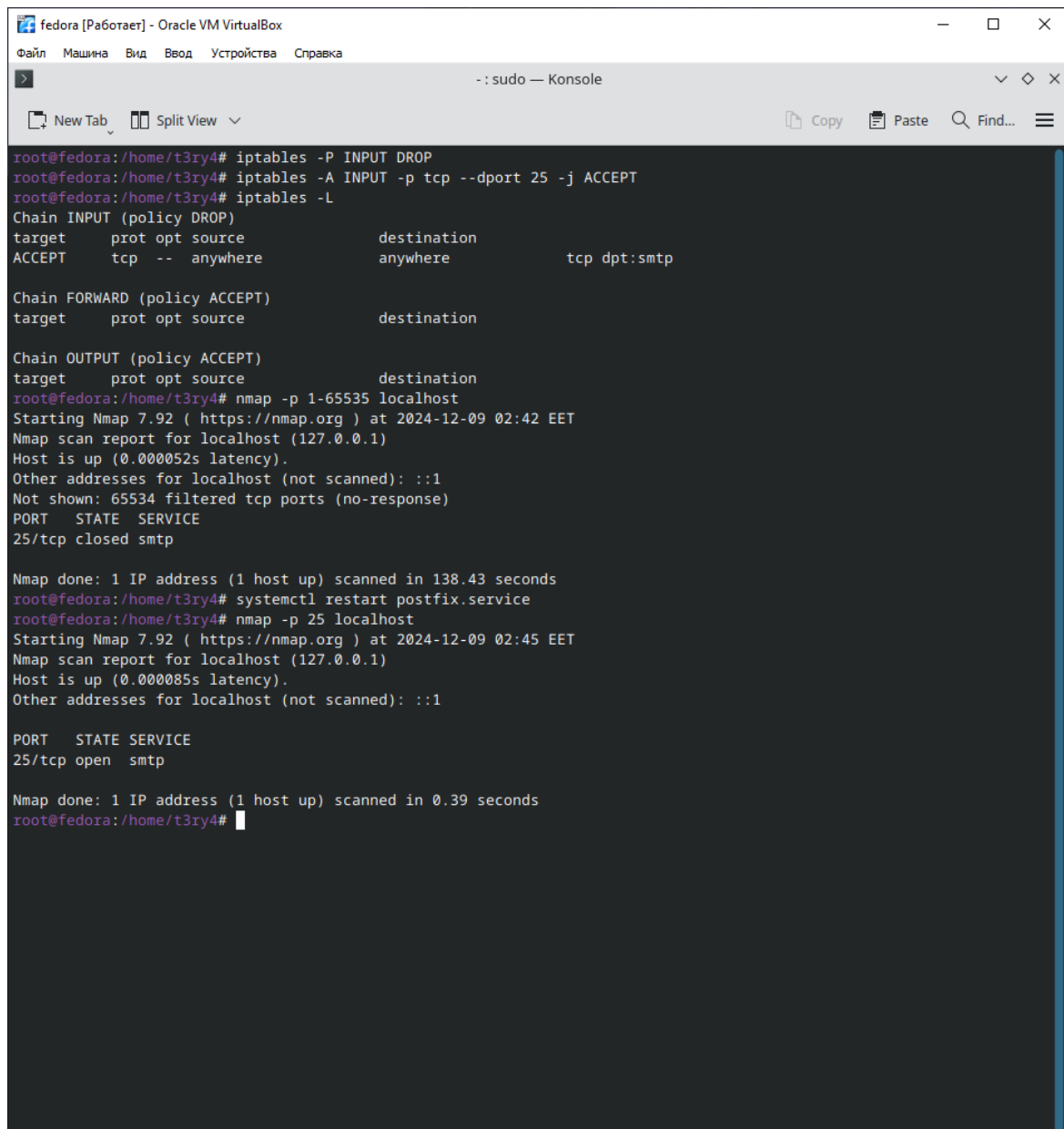


Рис. 3 – Відключення відповіді на ICMP-запити.



```
fedora [Работаєт] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

- : sudo — Konsole

New Tab  Split View  Copy  Paste  Find...

root@fedora:/home/t3ry4# iptables -P INPUT DROP
root@fedora:/home/t3ry4# iptables -A INPUT -p tcp --dport 25 -j ACCEPT
root@fedora:/home/t3ry4# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            tcp dpt:smtp
ACCEPT     tcp  --  anywhere              anywhere               tcp dpt:smtp

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@fedora:/home/t3ry4# nmap -p 1-65535 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-09 02:42 EET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000052s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    closed smtp

Nmap done: 1 IP address (1 host up) scanned in 138.43 seconds
root@fedora:/home/t3ry4# systemctl restart postfix.service
root@fedora:/home/t3ry4# nmap -p 25 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-09 02:45 EET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000085s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE
25/tcp    open  smtp

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@fedora:/home/t3ry4#
```

Рис. 4 – Закриття всіх портів, окрім SMTP.

```
root@fedora: /home/t3ry4# iptables -N spammsg
root@fedora: /home/t3ry4# iptables -A spammsg -s 192.168.88.249 -j DROP
root@fedora: /home/t3ry4# iptables -A spammsg -j RETURN
root@fedora: /home/t3ry4# iptables -A INPUT -j spammsg
root@fedora: /home/t3ry4# iptables -P INPUT ACCEPT
root@fedora: /home/t3ry4# ifconfig
ethp83: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.88.250 netmask 255.255.255.0 broadcast 192.168.88.255
    inet6 fe80::29be:fb1:9eb:374e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dc:6e:cd txqueuelen 1000 (Ethernet)
    RX packets 21966 bytes 15665994 (14.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6568 bytes 515607 (503.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 131385 bytes 5786416 (5.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 131385 bytes 5786416 (5.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@fedora: /home/t3ry4#
```

```
t3ry4@fedora:~$ ifconfig
ethp83: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.88.249 netmask 255.255.255.0 broadcast 192.168.88.255
    inet6 fe80::29be:fb1:9eb:374e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dc:6e:cd txqueuelen 1000 (Ethernet)
    RX packets 21966 bytes 15665994 (14.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6568 bytes 515607 (503.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 90 bytes 8236 (8.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 90 bytes 8236 (8.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

t3ry4@fedora:~$ ping -c 4 192.168.88.250
PING 192.168.88.250 (192.168.88.250) 56(84) bytes of data:
^C
--- 192.168.88.250 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3856ms

t3ry4@fedora:~$
```

```
Administration C:\Windows\system32\cmd.exe
C:\Users\t3ry4>ping 192.168.88.250

Pinging 192.168.88.250 with 32 bytes of data:
Reply from 192.168.88.250: bytes=32 time=1ms TTL=64
Reply from 192.168.88.250: bytes=32 time=1ms TTL=64
Reply from 192.168.88.250: bytes=32 time=1ms TTL=64
Reply from 192.168.88.250: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.88.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\t3ry4>
```

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.