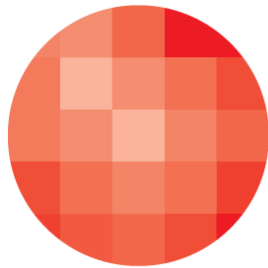


WARSZAWSKA WYŻSZA SZKOŁA INFORMATYKI
SYSTEMY OPERACYJNE



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

SPRAWOZDANIE NR 3 TEMAT:

Instalacja i konfiguracja roli NAT w
systemie Ubuntu Server

Wykonał
Wojciech Wiącek

1 Podstawy Teoretyczne

1.1 Polecenia do diagnostyki sieciowej:

1.1.1 Dig

Polecenie "dig" służy do przeprowadzania różnych rodzajów zapytań DNS, takich jak zapytania o rekordy DNS, serwery nazw, informacje o strefach DNS i wiele innych. W zależności od wykorzystanych parametrów, polecenie dig może zwrócić różne informacje, takie jak adresy IP, informacje o serwerach DNS, czasy odpowiedzi i inne.

1.1.2 Traceroute

polecenie "traceroute" w systemie Linux Ubuntu jest narzędziem wiersza poleceń, które służy do śledzenia trasy pakietów sieciowych między lokalnym komputerem a określonym adresem IP. Polecenie "traceroute" działa poprzez wysyłanie specjalnych pakietów sieciowych, tzw. pakietów ICMP, z kolejnymi wartościami "TTL" (Time To Live) na adres docelowy. Każdy ruter na trasie, przez który przechodzi pakiet, zmniejsza wartość TTL o jeden. Gdy wartość TTL osiągnie zero, ruter odrzuca pakiet i wysyła informację zwrotną (tzw. ICMP Time Exceeded Message) z powrotem do nadawcy. Dzięki temu można śledzić drogę, jaką pakiet musi przejść, aby dotrzeć do docelowego hosta.

1.2 Czym jest iptables

Iptables działa jako narzędzie wywoływane z poziomu wiersza poleceń, a jego zadaniem jest filtrowanie ruchu sieciowego, przekierowywanie pakietów między interfejsami sieciowymi oraz translacja adresów sieciowych (NAT). Iptables jest stosowane do konfiguracji firewall w systemach Linux i jest jednym z najczęściej używanych narzędzi do tego celu. Reguły firewalla definiowane za pomocą Iptables składają się z zestawów warunków, określających jakie pakiety powinny być blokowane, przepuszczane lub przekierowywane między interfejsami sieciowymi. Każda reguła jest definiowana na podstawie kilku parametrów, takich jak adres źródłowy, adres docelowy, porty itp.

1.3 Czym jest łańcuch w iptables

to sekwencja reguł filtrujących ruch sieciowy, które zostały zdefiniowane dla określonej kategorii ruchu. Każdy łańcuch definiuje, co ma się stać z pakietami, które spełniają warunki określone w regułach łańcucha. W systemie Iptables istnieją trzy łańcuchy, w których można definiować reguły filtracji ruchu:

- Chain INPUT: łańcuch ten definiuje reguły filtracji dla ruchu przychodzącego do systemu.
- Chain OUTPUT: łańcuch ten definiuje reguły filtracji dla ruchu wychodzącego z systemu.
- Chain FORWARD: łańcuch ten definiuje reguły filtracji dla ruchu przekazywanego przez system (ruch tranzytowy).

Każda reguła może określać, co ma się stać z pakietami, które spełniają warunki reguły, np. czy pakiet ma być odrzucony, przepuszczony lub przekierowany do innego łańcucha. Reguły łańcuchów są przetwarzane w kolejności zdefiniowanej przez użytkownika. Gdy pakiet trafia do łańcucha, kolejno przetwarzane są wszystkie reguły zdefiniowane w tym łańcuchu, aż do momentu, gdy zostanie znaleziona reguła, która określa, co ma się stać z pakietem. W przypadku, gdy żadna reguła nie określa dalszych działań, pakiet jest przetwarzany zgodnie z polityką domyślną, która zwykle oznacza odrzucenie pakietu.

1.4 Czym jest reguła w iptables

Reguła w Iptables składa się z dwóch podstawowych elementów:

- Warunki: określają, jakie pakiety sieciowe mają zostać przetworzone przez regułę. Warunki te obejmują takie parametry jak adres źródłowy, adres docelowy, porty, protokół, interfejsy sieciowe, itp.
- Działanie: określa, co ma się stać z pakietami sieciowymi, które spełniają warunki reguły. Działania te mogą obejmować takie opcje jak odrzucenie pakietu, przepuszczenie go, przekierowanie do innego interfejsu sieciowego lub łańcucha iptables.

Reguły w Iptables są definiowane w ramach łańcuchów, takich jak INPUT, OUTPUT lub FORWARD. Każda reguła jest przetwarzana w kolejności zdefiniowanej przez użytkownika, aż do momentu, gdy zostanie znaleziona reguła, która określa, co ma się stać z pakietem.

1.5 Czym jest tabela w iptables

W Iptables, tabela to struktura danych, która służy do przechowywania reguł filtracji ruchu sieciowego. Każda tabela zawiera trzy lub pięć łańcuchów, w których są definiowane reguły filtracji.

- Istnieją trzy podstawowe tabele w Iptables:
- Tabela filter: jest to tabela domyślna w Iptables, która zawiera trzy łańcuchy: INPUT, OUTPUT i FORWARD. W tej tabeli definiuje się reguły filtrowania ruchu na podstawie adresów IP, portów i protokołów.
- Tabela nat: ta tabela zawiera dwa łańcuchy: PREROUTING i POSTROUTING. Tabela nat służy do manipulacji nagłówków pakietów i adresów IP, np. do przekierowywania ruchu sieciowego na inne adresy IP.
- Tabela mangle: ta tabela również zawiera pięć łańcuchów, w tym trzy podstawowe łańcuchy filter, ale dodatkowo zawiera dwa łańcuchy: PREROUTING i OUTPUT. Tabela mangle służy do manipulacji nagłówkami pakietów i parametrami pakietów.

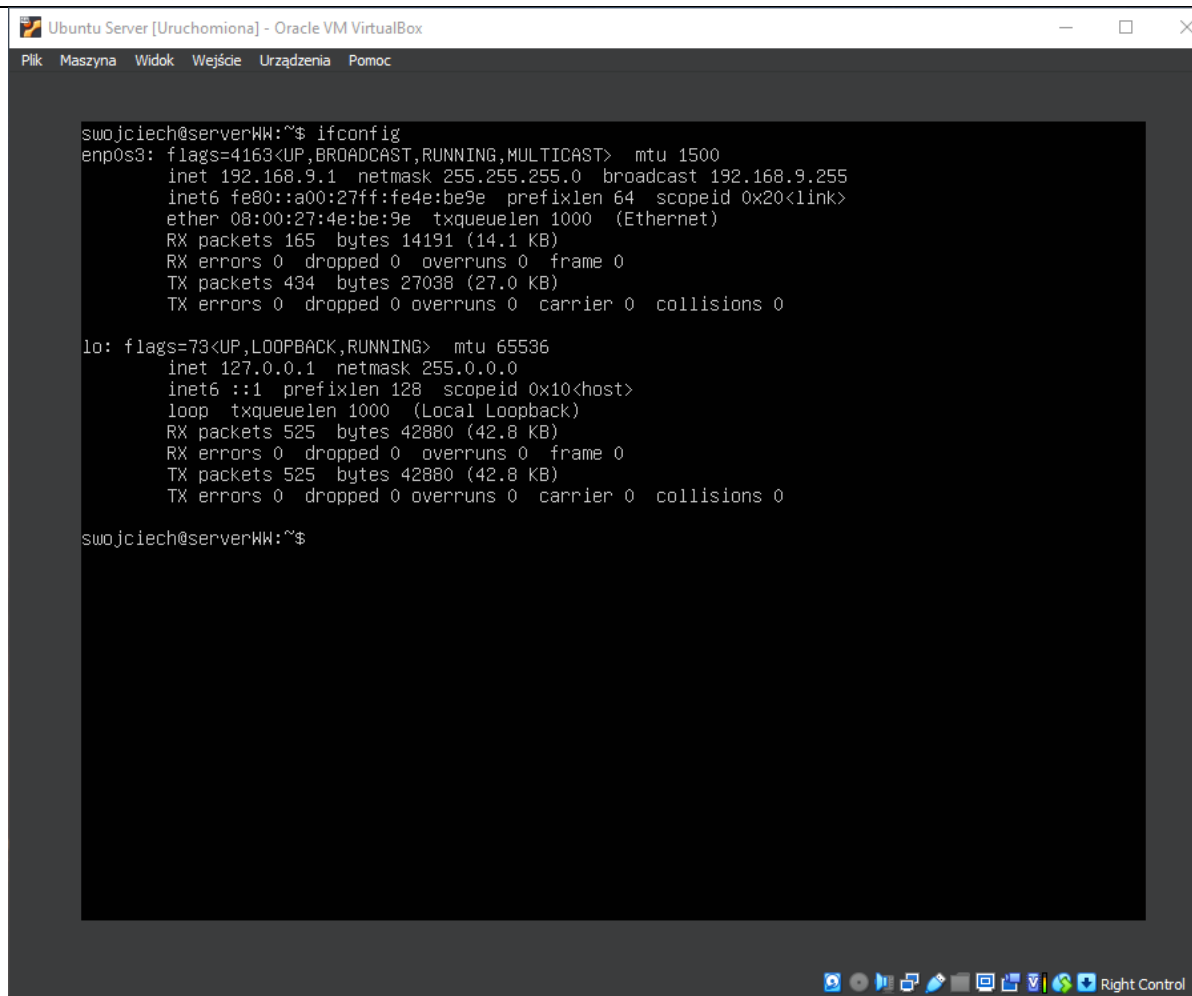
Dodatkowo, w niektórych dystrybucjach systemów Linux istnieją jeszcze dwie tabele:

- Tabela raw: ta tabela zawiera dwa łańcuchy: PREROUTING i OUTPUT. Tabela raw służy do manipulacji pakietami przed innymi tabelami.
- Tabela security: ta tabela jest związana z modułem SELinux i służy do filtrowania ruchu sieciowego na podstawie polityk bezpieczeństwa.

Każda tabela zawiera łańcuchy, które są przetwarzane w określonej kolejności, a reguły są definiowane w ramach tych łańcuchów. Po znalezieniu reguły, która pasuje do danego pakietu, zostaje podjęte odpowiednie działanie zdefiniowane w tej regule.

2 Przebieg czynności do realizacji zadania

Konfiguracja karty sieciowej serwera:



```
swojciech@serverWW:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.1 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::a00:27ff:fe4e:be9e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:4e:be:9e txqueuelen 1000 (Ethernet)
    RX packets 165 bytes 14191 (14.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 434 bytes 27038 (27.0 KB)
    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 525 bytes 42880 (42.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 525 bytes 42880 (42.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

swojciech@serverWW:~$
```

Ubuntu Server [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.9.1/24]
      gateway4: 192.168.9.1
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
    enp0s8:
      dhcp4: true
  version: 2

swojciech@serverWW:~$ sudo netplan apply
```

Right Control

```
Ubuntu Server [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

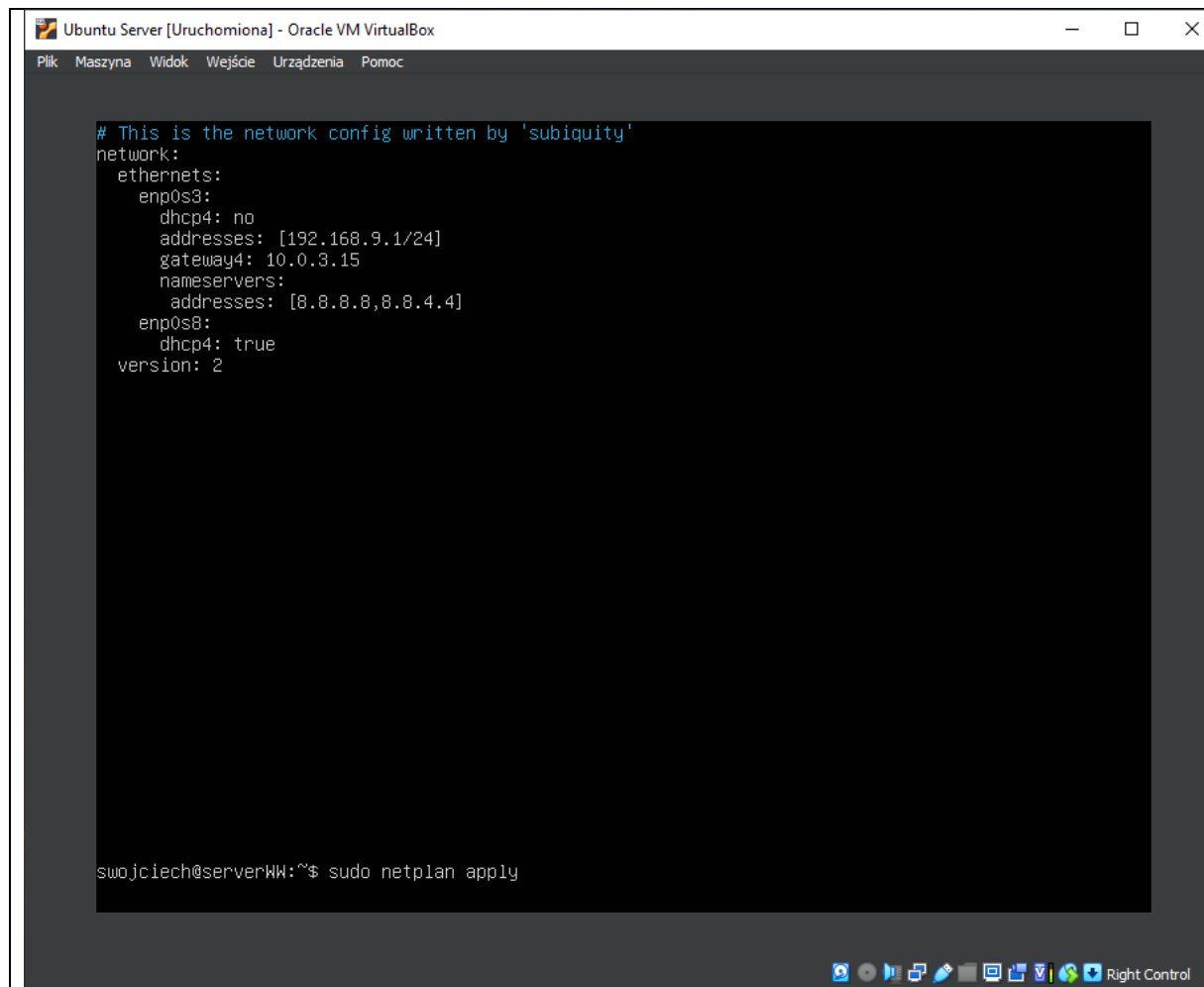
swojciech@serverWW:~$ sudo netplan apply
swojciech@serverWW:~$ sudo ifconfig

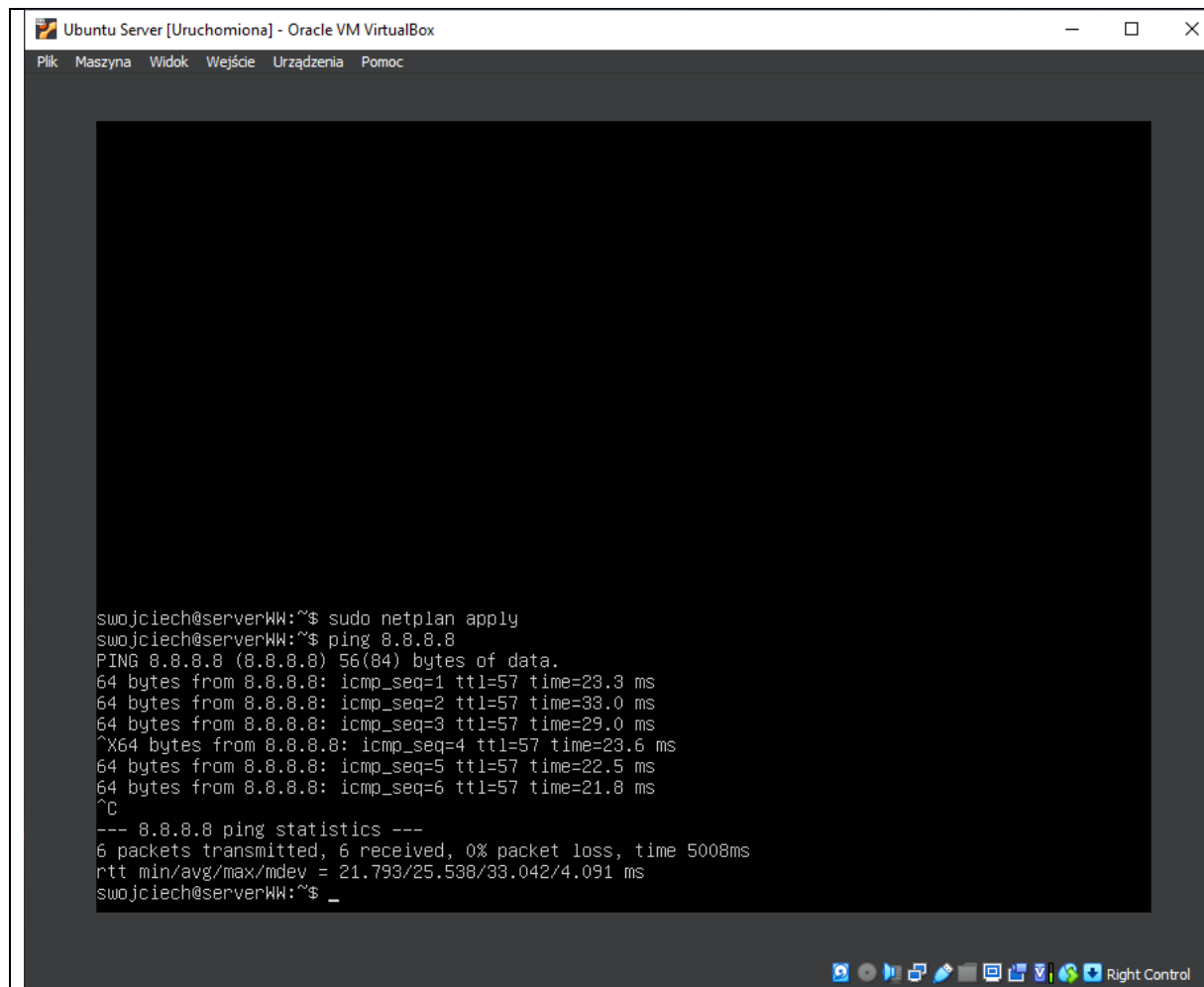
^Xenp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.1 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::a00:27ff:fe4e:be9e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:4e:be:9e txqueuelen 1000 (Ethernet)
    RX packets 286 bytes 23420 (23.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 949 bytes 58400 (58.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
    inet6 fe80::a00:27ff:feb6:314d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b6:31:4d txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 2420 (2.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2563 (2.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

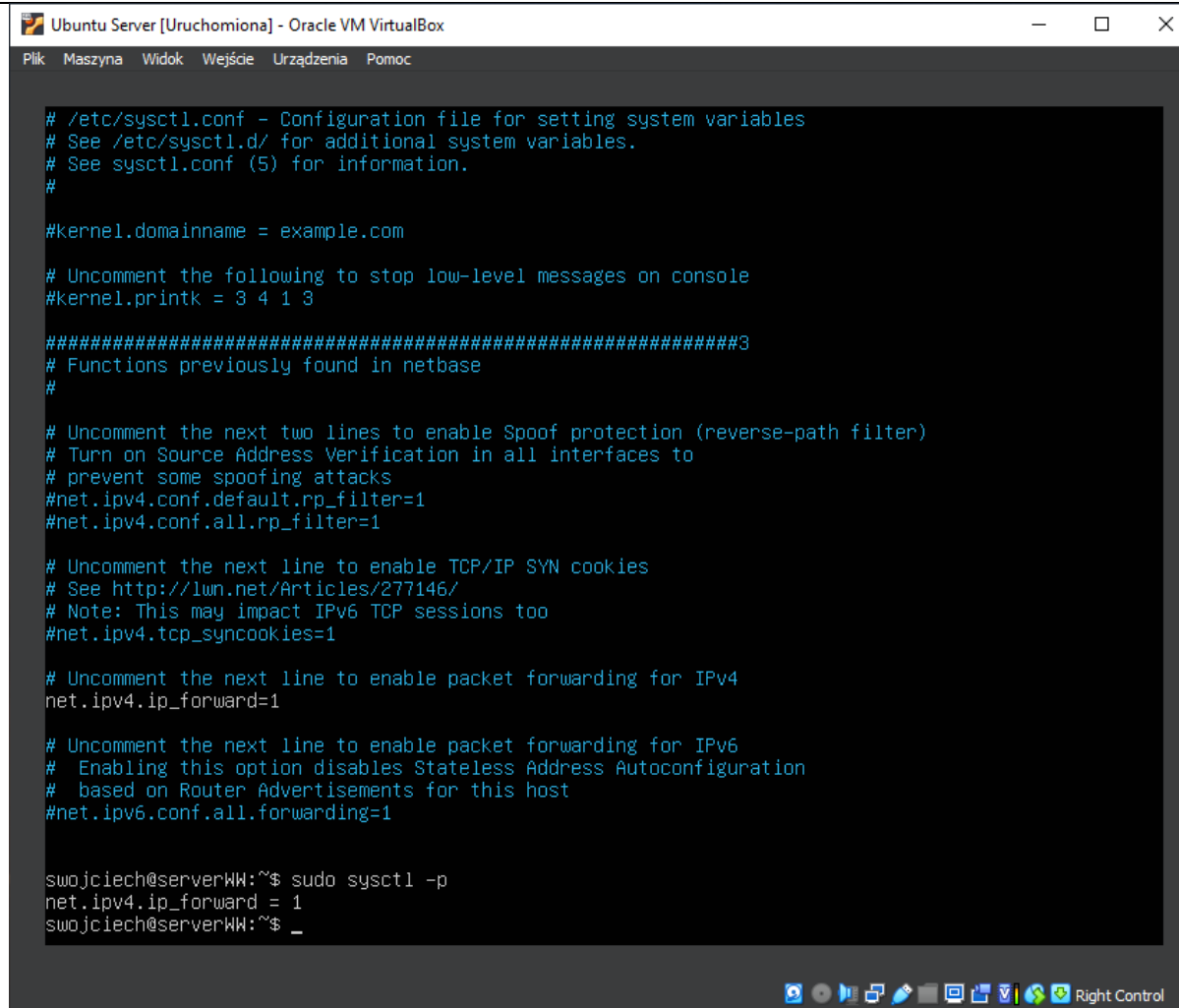
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1124 bytes 92219 (92.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1124 bytes 92219 (92.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

swojciech@serverWW:~$
swojciech@serverWW:~$ _
```





Edycja pliku sysctl.conf:



```
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
kernel.printk = 3 4 1 3

#####3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

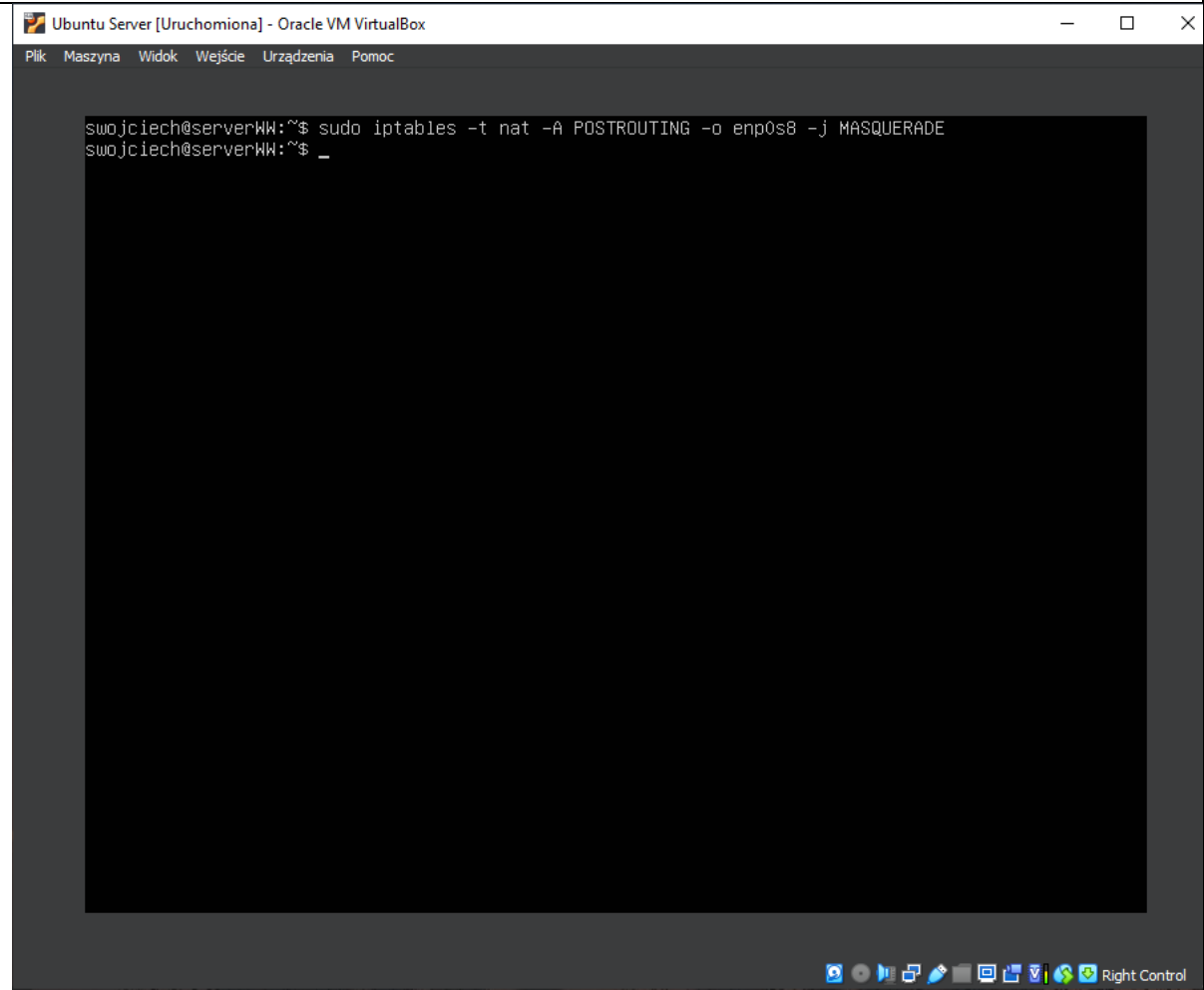
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
net.ipv6.conf.all.forwarding=1

swojciech@serverWM:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
swojciech@serverWM:~$ _
```

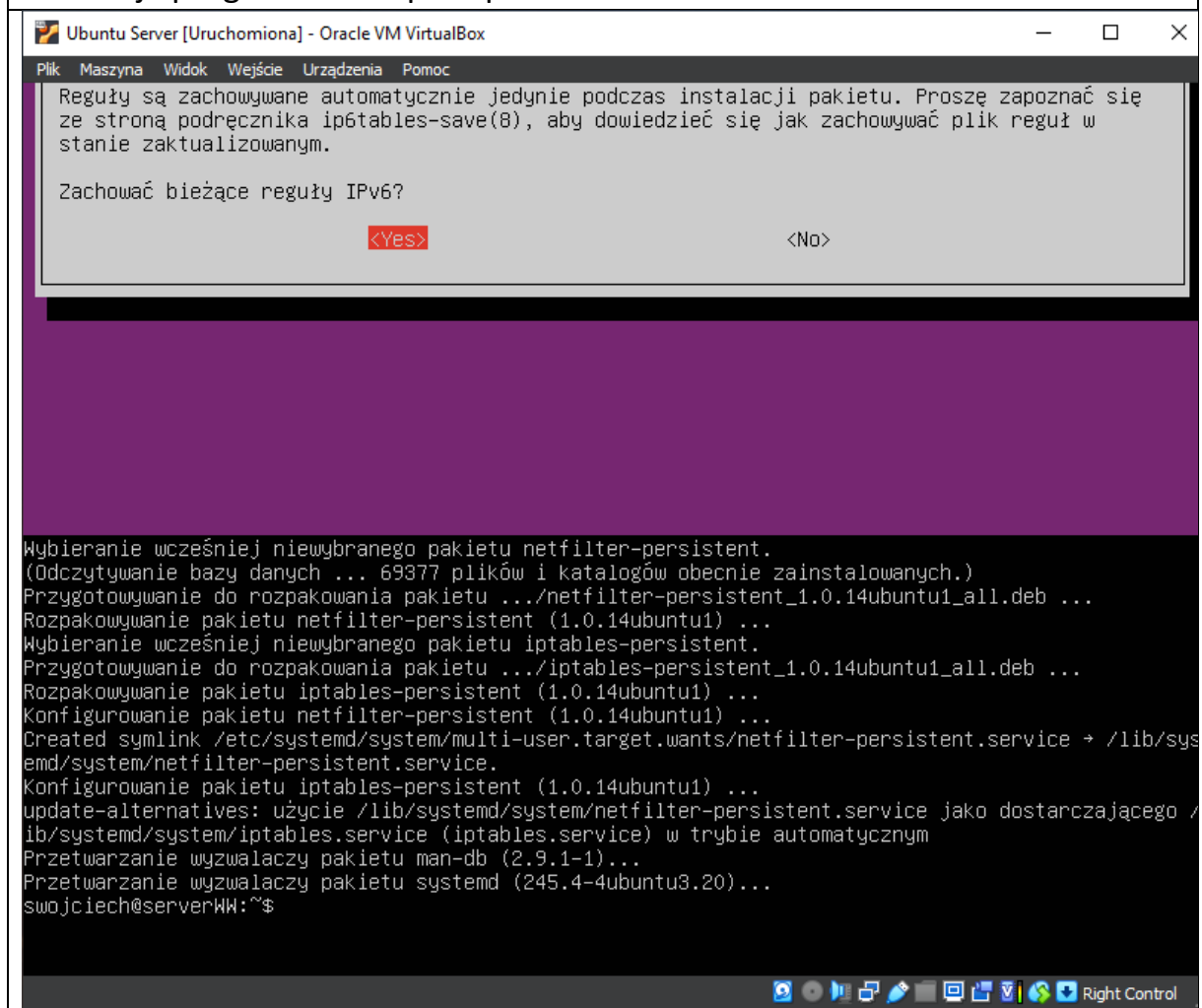
Nowy wpis tablicy routingu



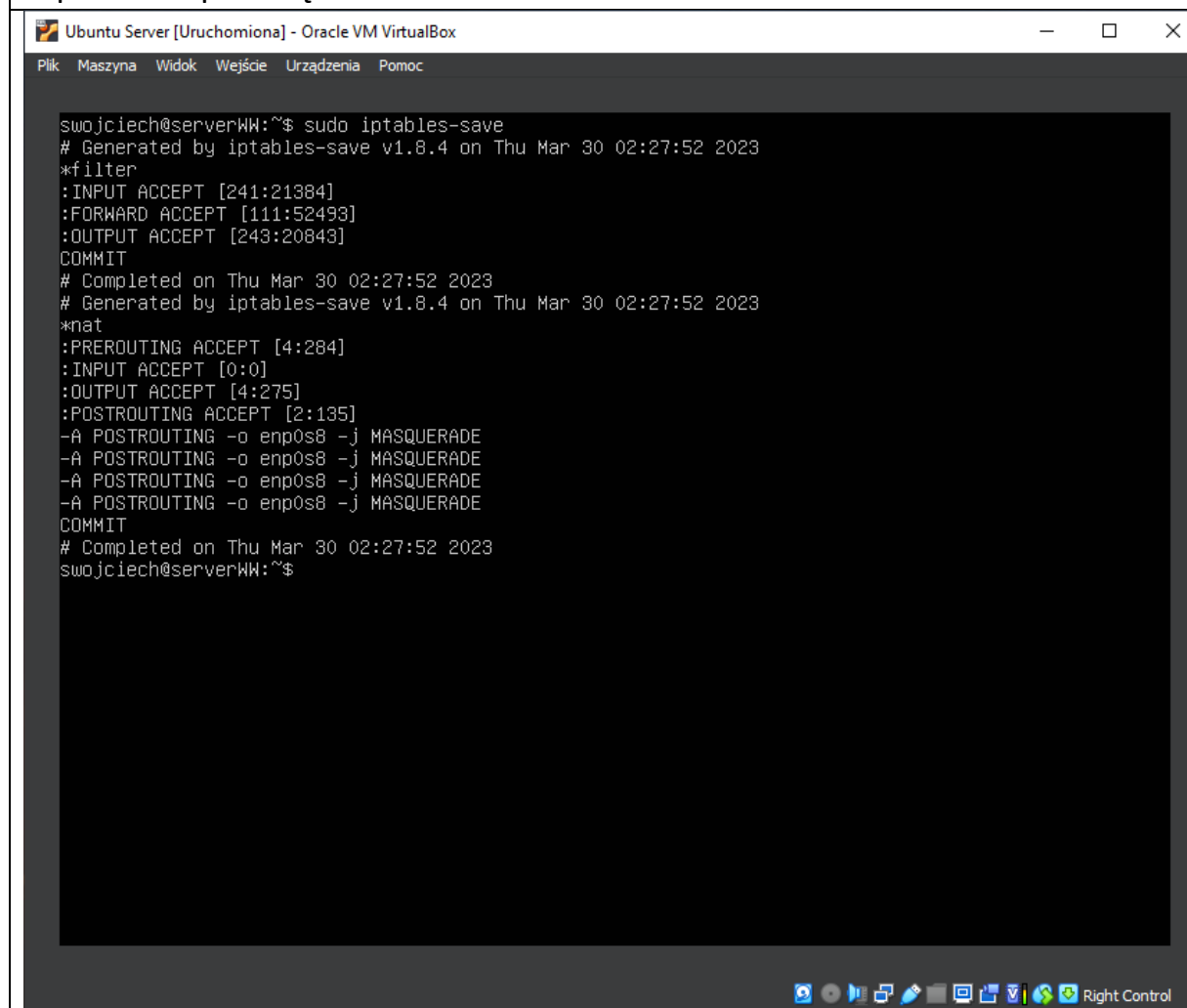
The screenshot shows a terminal window titled "Ubuntu Server [Uruchomiona] - Oracle VM VirtualBox". The window has a menu bar with "Plik", "Maszyna", "Widok", "Wejście", "Urządzenia", and "Pomoc". The terminal content shows the user "swojciech" at host "serverWW" in the home directory (~) executing the command "sudo iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE". The prompt changes to a root shell (#) after the command is executed. The terminal window has a dark background and a light gray border. At the bottom right, there is a "Right Control" button.

```
swojciech@serverWW:~$ sudo iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
swojciech@serverWW:~$ _
```

Instalacja programu do zapisu iptables

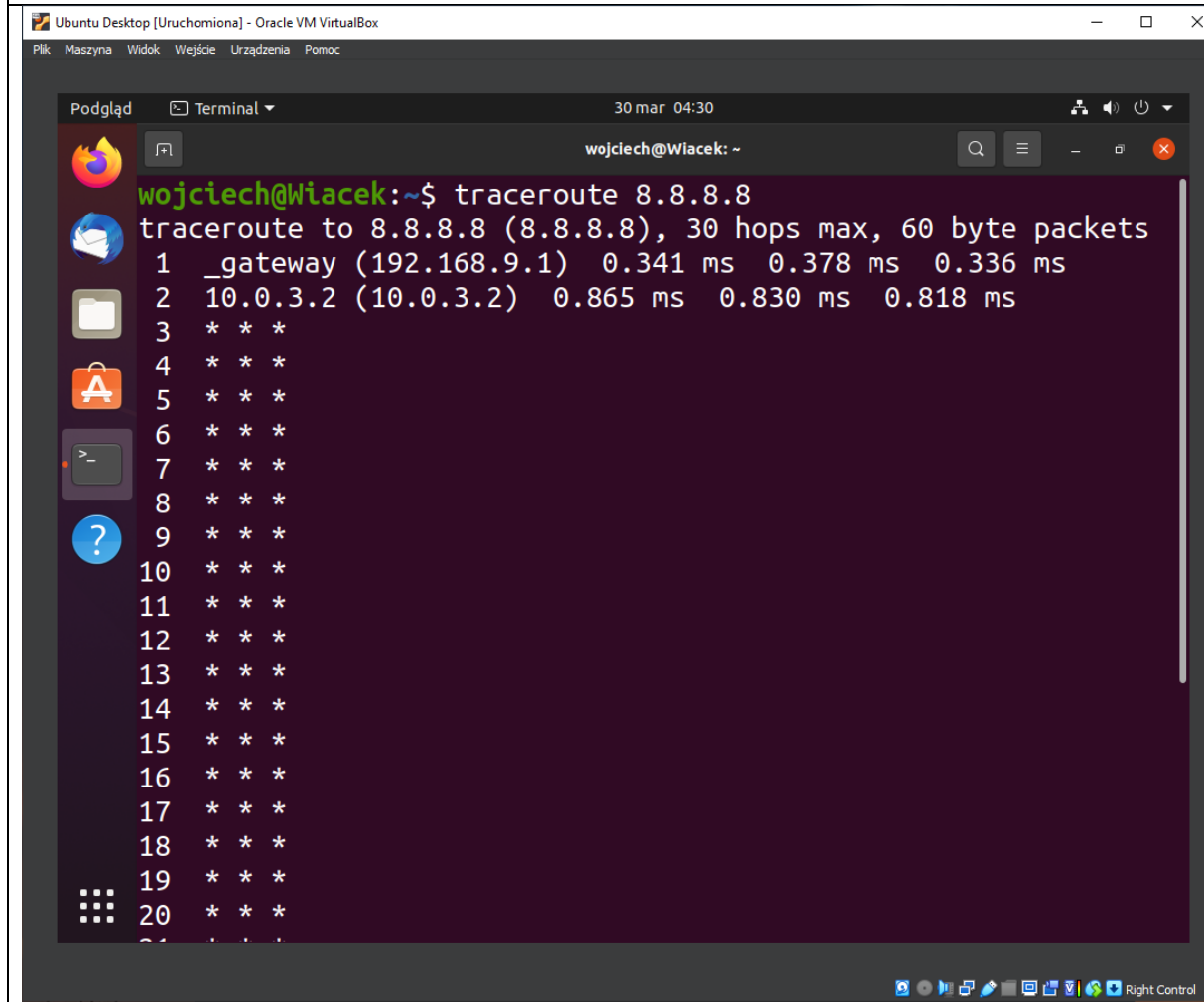


Wpis z masquaradą



```
swojciech@serverWW:~$ sudo iptables-save
# Generated by iptables-save v1.8.4 on Thu Mar 30 02:27:52 2023
*filter
:INPUT ACCEPT [241:21384]
:FORWARD ACCEPT [111:52493]
:OUTPUT ACCEPT [243:20843]
COMMIT
# Completed on Thu Mar 30 02:27:52 2023
# Generated by iptables-save v1.8.4 on Thu Mar 30 02:27:52 2023
*nat
:PREROUTING ACCEPT [4:284]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [4:275]
:POSTROUTING ACCEPT [2:135]
-A POSTROUTING -o enp0s8 -j MASQUERADE
-A POSTROUTING -o enp0s8 -j MASQUERADE
-A POSTROUTING -o enp0s8 -j MASQUERADE
-A POSTROUTING -o enp0s8 -j MASQUERADE
COMMIT
# Completed on Thu Mar 30 02:27:52 2023
swojciech@serverWW:~$
```

Sprawdzenie z poleceniem traceroute:



The screenshot shows a terminal window titled "wojciech@Wiacek: ~" with a dark purple background. The command `traceroute 8.8.8.8` has been executed. The output shows the path from the local machine to 8.8.8.8, with the first two hops providing IP addresses and round-trip times. Hops 3 through 20 show asterisks, indicating that the traceroute failed to reach the destination beyond the second hop.

```
wojciech@Wiacek:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.9.1)  0.341 ms  0.378 ms  0.336 ms
 2  10.0.3.2 (10.0.3.2)  0.865 ms  0.830 ms  0.818 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
```

3 Wnioski

Po dzisiejszym ćwiczeniu nauczyłem się tworzyć i konfigurować serwer NAT w systemie linux ubuntu. Dowiedziałem się czym jest tablica 'iptables'. Wszystko było bardzo proste i przyjemne, uważam że konfiguracja tej roli serwera jest łatwiejsza na tym systemie w porównaniu do systemu Windows serwer, pomimo tego że nie posiadamy trybu graficznego. Jediną trudność sprawiło mi od komentowanie niewłaściwej linijki w pliku konfiguracyjnym sysctl.conf lecz gdy znalazłem błąd wszystko zaczęło działać