

10. Zapora sieciowa (firewall) I sterowanie ruchem sieciowym

- Stan 4 Wirtualnych maszyn jest przed zmianą ip w VM1 na 10.1.2.105 jak I zmianą w VM3 w 40-network-cfg

1. iptables

a) status:

```
vm1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm1:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
root@vm1:~# _

vm2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm2:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
root@vm2:~# _

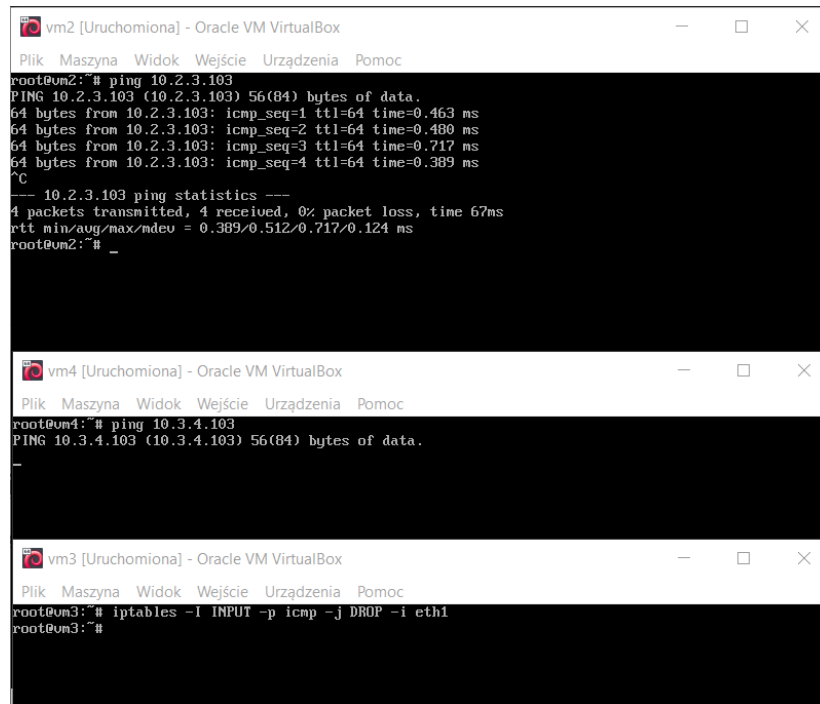
vm3 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm3:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
root@vm3:~# _

vm4 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm4:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
root@vm4:~# _
```

- b) jest możliwość połączenia się ssh, ale wymaga hasła do sterowania, nie jest to ani hasło użytkownika debian, ani podstawowe hasło "toor" # okazało się że łącząc się jako root chce się połączyć automatycznie na użytkownika root, co nie jest wykonywalne
- c) z braku możliwości zalogowania się, nie było potrzeby wyjścia

```
vm4 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm4:~# ping 10.3.4.103
PING 10.3.4.103 (10.3.4.103) 56(84) bytes of data:
64 bytes from 10.3.4.103: icmp_seq=1 ttl=64 time=0.448 ms
64 bytes from 10.3.4.103: icmp_seq=2 ttl=64 time=0.538 ms
64 bytes from 10.3.4.103: icmp_seq=3 ttl=64 time=0.399 ms
64 bytes from 10.3.4.103: icmp_seq=4 ttl=64 time=0.518 ms
64 bytes from 10.3.4.103: icmp_seq=5 ttl=64 time=0.349 ms
64 bytes from 10.3.4.103: icmp_seq=6 ttl=64 time=0.556 ms
^C
--- 10.3.4.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 111ms
rtt min/avg/max/mdev = 0.349/0.468/0.556/0.075 ms
root@vm4:~# ssh 10.3.4.103
The authenticity of host '10.3.4.103 (10.3.4.103)' can't be established.
ECDSA key fingerprint is SHA256:CQkz6stqAKI/38Acnax3uAtHFXpcUbFHWd7qdM6c2w.
Are you sure you want to continue connecting (yes/no)? yes
Please type 'yes' or 'no': yes
Warning: Permanently added '10.3.4.103' (ECDSA) to the list of known hosts.
root@10.3.4.103's password:
Permission denied, please try again.
root@10.3.4.103's password:
Permission denied, please try again.
root@10.3.4.103's password:
root@10.3.4.103: Permission denied (publickey,password).
root@vm4:~#
```

- d) .
e) .



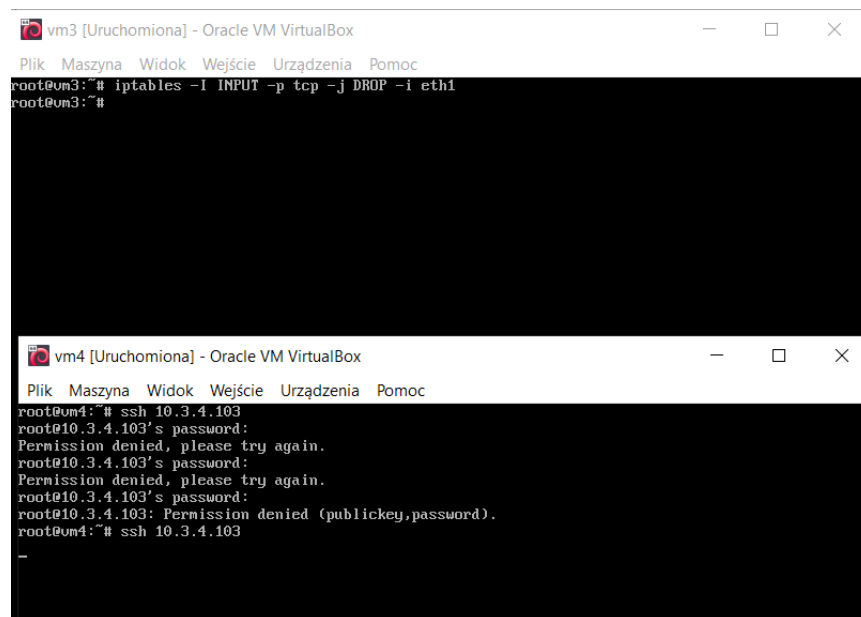
The image shows three stacked terminal windows from Oracle VM VirtualBox. The top window, titled 'vm2 [Uruchomiona]', shows a ping command from root@vm2 to 10.2.3.103, displaying four successful ICMP packets with varying times. The middle window, titled 'vm4 [Uruchomiona]', shows a ping command from root@vm4 to 10.3.4.103, which is partially visible. The bottom window, titled 'vm3 [Uruchomiona]', shows the execution of the iptables command: 'iptables -I INPUT -p icmp -j DROP -i eth1'.

```
vm2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm2:~# ping 10.2.3.103
PING 10.2.3.103 (10.2.3.103) 56(84) bytes of data:
64 bytes from 10.2.3.103: icmp_seq=1 ttl=64 time=0.463 ms
64 bytes from 10.2.3.103: icmp_seq=2 ttl=64 time=0.480 ms
64 bytes from 10.2.3.103: icmp_seq=3 ttl=64 time=0.717 ms
64 bytes from 10.2.3.103: icmp_seq=4 ttl=64 time=0.389 ms
^C
--- 10.2.3.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 67ms
rtt min/avg/max/mdev = 0.389/0.512/0.717/0.124 ms
root@vm2:~# _

vm4 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm4:~# ping 10.3.4.103
PING 10.3.4.103 (10.3.4.103) 56(84) bytes of data.
-

vm3 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm3:~# iptables -I INPUT -p icmp -j DROP -i eth1
root@vm3:~#
```

- f) w wcześniej podanej komendzie wymagana była zmiana z "icmp" na "tcp"

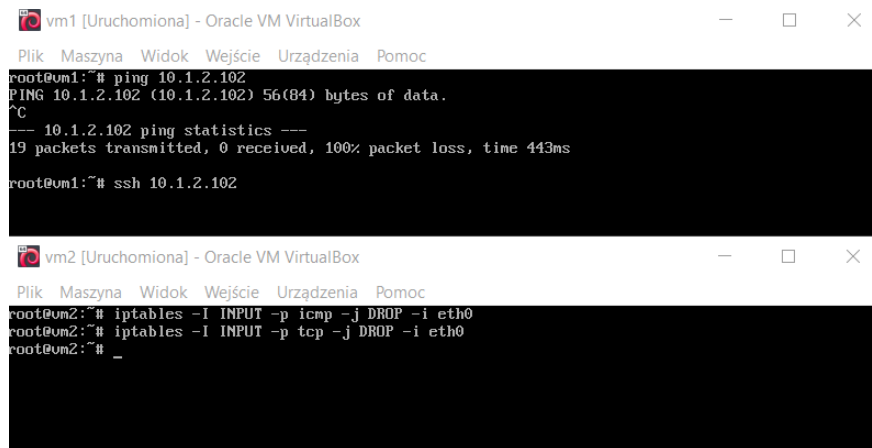


The image shows two stacked terminal windows from Oracle VM VirtualBox. The top window, titled 'vm3 [Uruchomiona]', shows the execution of the iptables command: 'iptables -I INPUT -p tcp -j DROP -i eth1'. The bottom window, titled 'vm4 [Uruchomiona]', shows an attempt to connect via ssh from root@vm4 to 10.3.4.103, which fails with 'Permission denied' for both password and public key authentication.

```
vm3 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm3:~# iptables -I INPUT -p tcp -j DROP -i eth1
root@vm3:~#

vm4 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm4:~# ssh 10.3.4.103
root@10.3.4.103's password:
Permission denied, please try again.
root@10.3.4.103's password:
Permission denied, please try again.
root@10.3.4.103's password:
root@10.3.4.103: Permission denied (publickey,password).
root@vm4:~# ssh 10.3.4.103
-
```

g) .

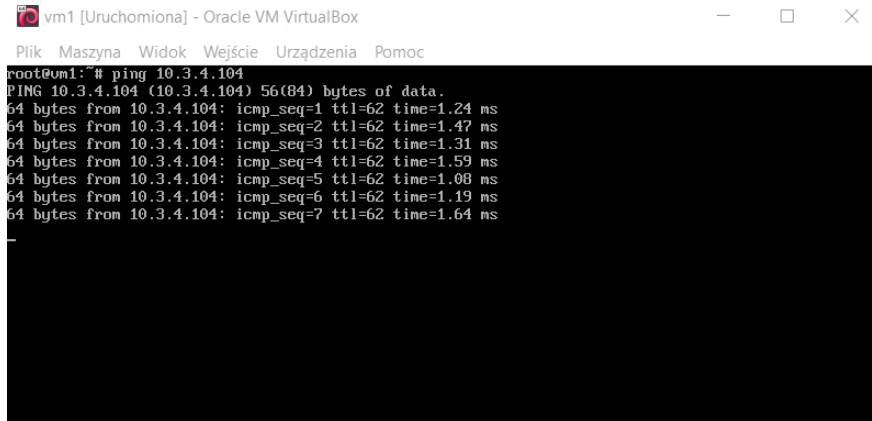


```
vm1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm1:~# ping 10.1.2.102
PING 10.1.2.102 (10.1.2.102) 56(84) bytes of data:
^C
--- 10.1.2.102 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 443ms

root@vm1:~# ssh 10.1.2.102

vm2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm2:~# iptables -I INPUT -p icmp -j DROP -i eth0
root@vm2:~# iptables -I INPUT -p tcp -j DROP -i eth0
root@vm2:~# _
```

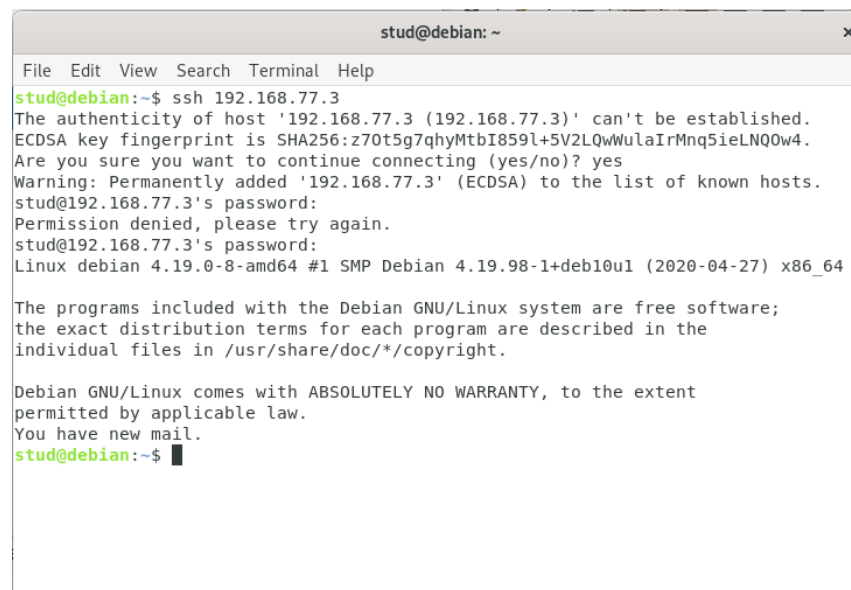
h) ping jest możliwy między VM1 i VM4



```
vm1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@vm1:~# ping 10.3.4.104
PING 10.3.4.104 (10.3.4.104) 56(84) bytes of data:
64 bytes from 10.3.4.104: icmp_seq=1 ttl=62 time=1.24 ms
64 bytes from 10.3.4.104: icmp_seq=2 ttl=62 time=1.47 ms
64 bytes from 10.3.4.104: icmp_seq=3 ttl=62 time=1.31 ms
64 bytes from 10.3.4.104: icmp_seq=4 ttl=62 time=1.59 ms
64 bytes from 10.3.4.104: icmp_seq=5 ttl=62 time=1.08 ms
64 bytes from 10.3.4.104: icmp_seq=6 ttl=62 time=1.19 ms
64 bytes from 10.3.4.104: icmp_seq=7 ttl=62 time=1.64 ms
```

2. ufw

- a) moje ip 192.168.77.3/24
- b) połączenie było niemożliwe z poziomu root'a, natomiast było to wykonywalne z poziomu stud. Prawdopodobnie również by to zadziało między VM1



```
stud@debian: ~
File Edit View Search Terminal Help
stud@debian:~$ ssh 192.168.77.3
The authenticity of host '192.168.77.3 (192.168.77.3)' can't be established.
ECDSA key fingerprint is SHA256:z70t5g7qhyMtbI859l+5V2LQwWulaIrMnq5ieLNQ0w4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.77.3' (ECDSA) to the list of known hosts.
stud@192.168.77.3's password:
Permission denied, please try again.
stud@192.168.77.3's password:
Linux debian 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
stud@debian:~$
```

- c) zostały wprowadzone komendy na domyślne zablokowanie wszystkiego wchodzącego i odblokowanie na wszystkie wychodzące
- d) połączenie ssh zostało zablokowane

```
stud@debian: ~  
File Edit View Search Terminal Help  
stud@debian:~$ sudo -i  
root@debian:~# ufw enable  
Firewall is active and enabled on system startup  
root@debian:~# logout  
stud@debian:~$ ssh 192.168.77.3
```

- e) .
- f) jest możliwe połączenie przez ssh

```
stud@debian: ~  
File Edit View Search Terminal Help  
root@debian:~# ufw allow from 192.168.77.3/24 to any port 22  
WARN: Rule changed after normalization  
Rule added  
root@debian:~# logout  
stud@debian:~$ ssh 192.168.77.3  
stud@192.168.77.3's password:  
Permission denied, please try again.  
stud@192.168.77.3's password:  
Linux debian 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
Last login: Thu May 14 19:18:35 2020 from 192.168.77.3  
stud@debian:~$ sudo -i  
[sudo] password for stud:  
root@debian:~# ufw status  
Status: active  
  
To Action From  
--  
22 ALLOW 192.168.77.0/24  
  
root@debian:~#
```

- g) http to port 80
https to port 443
pojawiły się nowe reguły
- h) .

```

stud@debian: ~
File Edit View Search Terminal Help
root@debian:~# ufw deny out 80
Rule added
Rule added (v6)
root@debian:~# ufw deny out 443
Rule added
Rule added (v6)
root@debian:~# ufw status
Status: active

To Action From
--
22 ALLOW 192.168.77.0/24

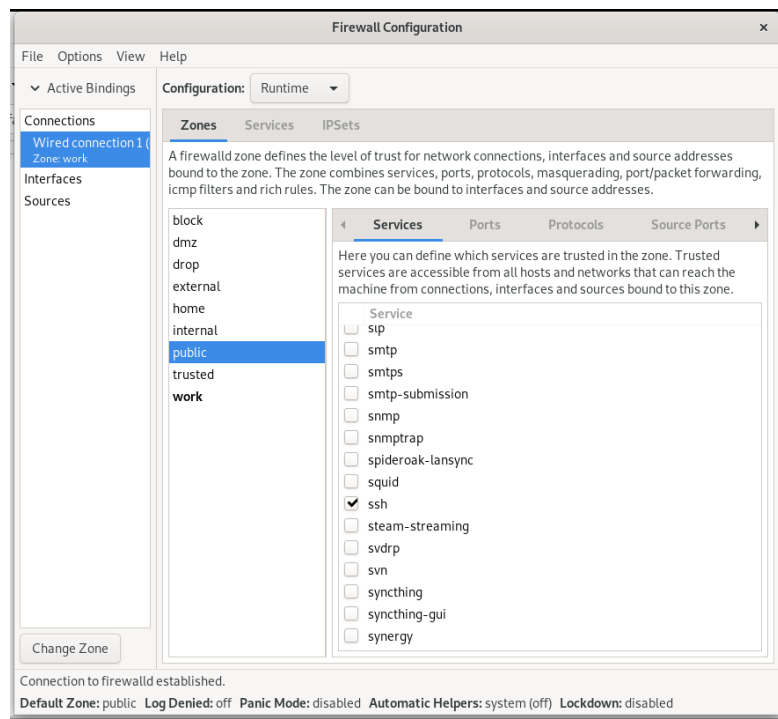
80 DENY OUT Anywhere
443 DENY OUT Anywhere
80 (v6) DENY OUT Anywhere (v6)
443 (v6) DENY OUT Anywhere (v6)

root@debian:~# apt-get purge ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  girl.2-totem-1.0 hyphen-en-us javascript-common libreoffice-help-common
  libreoffice-help-en-us libtotem0 mythes-en-us node-normalize.css
  totem-common
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  ufw*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 852 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 150524 files and directories currently installed.)
Removing ufw (0.36-1) ...
Processing triggers for man-db (2.8.5-2) ...
(Reading database ... 150431 files and directories currently installed.)
Purging configuration files for ufw (0.36-1) ...
Processing triggers for systemd (241-7-deb10u4) ...
Processing triggers for rsyslog (8.1901.0-1) ...
root@debian:~#

```

3. firewalld I firewall-applet

- a) ssh można używać na : work, public, internal, home, external i dmz



- b) jest możliwość połączenia z komputera fizycznego do VM

```
stud@debian: ~$ ping 192.168.77.3
Pinging 192.168.77.3 with 32 bytes of data:
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.77.3:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Uzytkownik>ssh stud@192.168.77.3
The authenticity of host '192.168.77.3 (192.168.77.3)' can't be established.
ECDSA key fingerprint is SHA256:z70t5g7ghyMtbI8591+5V2LQwWulaIrMnq5ieLNQOw4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.77.3' (ECDSA) to the list of known hosts.
stud@192.168.77.3's password:
Linux debian 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64
Linux debian 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu May 14 19:52:28 2020 from 192.168.77.3
stud@debian:~$
```

- c) połączenie ssh nie jest możliwe

```
Wiersz polecenia - ssh stud@192.168.77.3
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Uzytkownik>ping 192.168.77.3

Pinging 192.168.77.3 with 32 bytes of data:
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Uzytkownik>ssh stud@192.168.77.3
```

- d) pingowanie stało się niemożliwe, nie widziałem żadnych zachowań (powiadomień) na VM

```
Wiersz polecenia

Ping statistics for 192.168.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Użytkownik>ping 192.168.77.3

Pinging 192.168.77.3 with 32 bytes of data:
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64
Reply from 192.168.77.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Użytkownik>ping 192.168.77.3

Pinging 192.168.77.3 with 32 bytes of data:
Reply from 192.168.77.3: Destination host unreachable.
Reply from 192.168.77.3: Destination host unreachable.
Reply from 192.168.77.3: Destination host unreachable.
Reply from 192.168.77.3: Destination host unreachable.

Ping statistics for 192.168.77.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```