

# Raport z ćwiczenia 1.

Daniel Daczko (nr albumu: 299241)

Grupa I (poniedziałek 14.15)

14 maja 2020

## Spis treści

<b>1</b>	<b>Cel ćwiczenia</b>	<b>1</b>
<b>2</b>	<b>Realizacja ćwiczenia</b>	<b>1</b>
2.1	Protokół komunikacyjny SSH . . . . .	1
2.1.1	Logowanie poprzez SSH na maszynę VOLT . . . . .	2
2.1.2	Zmiana hasła do konta . . . . .	2
2.1.3	Wygenerowanie na VOLCIE kluczy SSH . . . . .	2
2.1.4	Wygenerowanie kluczy na maszynie domowej . . . . .	2
2.1.5	Eksport klucza publicznego z maszyny domowej na VOLT'a . . . . .	3
2.1.6	Sprawdzenie poprawności działania logowania bez hasła . . . . .	3
2.2	Kreacja maszyny wirtualnej FreeBSD 64-bit . . . . .	3
2.2.1	Pobranie obrazu systemu i instalacja . . . . .	3
2.2.2	Sprawdzenie dwóch wariantów konfiguracji sieci maszyny wirtualnej . . . . .	4
<b>3</b>	<b>Podsumowanie i wnioski</b>	<b>5</b>

## 1 Cel ćwiczenia

Celem ćwiczenia jest dokonanie pierwszego logowania na serwer `volt.zet.pw.edu.pl`, zmiana hasła użytkownika i wygenerowanie kluczy SSH zarówno na serwerze, jak i na maszynie domowej. Następnie wyeksportowanie i zaimportowanie klucza w taki sposób, aby można się było logować na serwer VOLT bez konieczności podawania hasła. Kolejnym etapem jest stworzenie maszyny wirtualnej opartej o system FreeBSD w wersji 64-bitowej i sprawdzenie dwóch wariantów konfiguracji sieci, tak aby możliwe było zalogowanie się na VOLT'a przez SSH.

## 2 Realizacja ćwiczenia

### 2.1 Protokół komunikacyjny SSH

W poniższych punktach przedstawię kolejno wykonywane przeze mnie kroki.

### 2.1.1 Logowanie poprzez SSH na maszynę VOLT

Do zalogowania się na maszynę VOLT użyłem następującego polecenia:

```
daniel@Daniels-MacBook-Pro % ssh daczkod@volt.zet.pw.edu.pl
```

Następnie wprowadziłem domyślne hasło. Po pomyślnym logowaniu, zapytany o sposób konfiguracji wybrałem opcję 0. W kolejnym kroku utworzyłem skrót do folderu labsk wykorzystując polecenie:

```
volt% ln -s /usr/local/zetis/labsk labsk
```

### 2.1.2 Zmiana hasła do konta

Moje nowe hasło to ciąg znaków zgodny z zaleceniami prowadzącego. W celu zmiany hasła posłużyłem się poleceniem:

```
volt% passwd
```

### 2.1.3 Wygenerowanie na VOLCIE kluczy SSH

W kolejnym kroku wygenerowałem klucze SSH na moim koncie serwera VOLT pozostawiając passphrase jako pusty ciąg, przy pomocy polecenia:

```
volt% ssh-keygen
```

```
[volt% cd .ssh ]
[volt% ls -la ]
total 1
drwx----- 2 daczkod stud 512 11 maj 14:28 .
drwx-----x 3 daczkod stud 512 11 maj 14:28 ..
-rw----- 1 daczkod stud 1679 11 maj 14:28 id_rsa
-rw-r--r-- 1 daczkod stud 408 11 maj 14:28 id_rsa.pub
[volt% cat id_rsa.pub ]
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQc+cX0ilioUfJQPXDNVn+wyVM7RY4bdxdArZUsdZnaJ
zEenyGeIC+B//Cc5M6omGt4H+wUmu9aI2YU/QokrLJgHywgYvemc7LswIbp13NiIUK0tOTRk5M9toq0D
w/NtH3rd4FUw27nQUR11Fey93L0DhWh9qczc9j3l8xCeX/zTKgHIGfU08b3kcHq48lX2y5MVJbRVRr5
AwsJ1mJSBa952DF4m3fF8GzYMU5t80D731zHgvW5Qtrmh/+pHHFxeBw1/oZHhw77zY10V6tAuS0yPuAt
hWhoJMA3+lZd0tajdeYeMEF4XRpfHX6JxYKe1RuJhVKBowbepK71todnXSEN daczkod@volt.zet.pw
.edu.pl
[volt% ]
```

### 2.1.4 Wygenerowanie kluczy na maszynie domowej

Korzystając z tego samego polecenia co w poprzednim kroku wygenerowałem klucze na maszynie domowej:

```
[daniel@Daniels-MacBook-Pro ~ % ssh-keygen ]
Generating public/private rsa key pair.
[Enter passphrase (empty for no passphrase): ]
[Enter same passphrase again: ]
Your identification has been saved in /Users/daniel/.ssh/id_rsa.
Your public key has been saved in /Users/daniel/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:r4XleEutFuR8ONT6g6Ha2ix0EnW08RdrHm1kIIRxoo daniel@Daniels-MacBook-Pro.lo
cal
The key's randomart image is:
+---[RSA 3072]-----+
|      .++ .o.o |
|      .o .oo. o |
|      . .oo. .oo |
|      E .o oo.o.. |
|      +S...* .. |
|      . +* = = |
|      .o+0 0 |
|      +=.X . |
|      ...=oo |
+---[SHA256]-----+
[daniel@Daniels-MacBook-Pro ~ % cat .ssh/id_rsa.pub ]
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcCcPcwJQRkM4TXrLfBew0QdgDut63LuM84C9pPk
s1jgEeqm31/dXKtW0J253WwGUeF11xNeSEI106/XhL7Lbtvzf+YQGiBy36rWafP1tJuf93cdPhIwWM4B
YJScSLCc6iBBZgkUapvxEc5+MqHmA92CdB1HdBNWKubo17XT9de0r/HxCoC/6fgCf+ye5PV1ogJJjQ
uV1Q3JYt2Zts6/dmldnIhswfyzVTJUsLTMluZQ1vMXgyqGjXEKCM6CWTNWAHeTf8CdLrV1t8Qo1T4z9
cTja3W61RZM6d07800kgZeN8rQPvTIDumMrgZK5D7ozNMWels3DbLJ1wYu4GMPBDefu8g0qfpQV8GeU
oEMvTFRfd1/TC8/51R9U42v4+wKpAAMqmFhvUoy3FqouzIqk+fY1sax7gT5MnuFF/sy5RND/+Zetr2+S
mvxYNBZ0gjo2dLzL/IFiz9NrIrYbNYgCBQXqmDwokaAigxyd/BEPfGXUhrmS5T9LHKaLYaZs= daniel@
Daniels-MacBook-Pro.local
```

## 2.1.5 Eksport klucza publicznego z maszyny domowej na VOLT'a

Do wyeksportowania klucza publicznego użyłem polecenia:

```
daniel@Daniels-MacBook-Pro % cat .ssh/id_rsa.pub | ssh daczkod@volt.zet.pw.edu.pl 'cat ->
.ssh/authorized_keys'
```

## 2.1.6 Sprawdzenie poprawności działania logowania bez hasła

Następnie podjąłem próbę logowania bez hasła, która powiodła się pomyślnie:

```
[daniel@Daniels-MacBook-Pro ~ % ssh daczkod@volt.iem.pw.edu.pl ]
Last login: Mon May 11 15:41:23 2020 from 185.152.123.138
Want to know how many words, lines, or bytes are contained in a file? Type
"wc filename".
-- Dru <genesis@istar.ca>
Podniesione systemy dla LabSK: s0,s1,s4: Ubuntu, s2,s3,s6: FreeBSD, s5,s6: Core0
S (Docker)
[volt% cd .ssh ]
[volt% cat authorized_keys ]
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC1ccpCwJQrRkM4TxRlfbew0QdgDutf63LuM84C9pPk
s1jqEeqm31/dXKtW0J253WvGuEFi1xNeSEI106/XhL7Lbtvzf+YQGiBy36rWafLtJUf93cdPhIwWM4B
YJScSLCcGiBBZgkUapveXEc5+MqHmA92CdB1HdBNKuboj17XT9de0r/HxCoC/6fgCf+ye5PVlogJJjq
uV1Q3JYt2Zts6/dmldnIhsWfyZVTJUsLTmLuZQ1vMXgyqaGjXEKCM6CWTNWAHeTf8CdLrV1t8Qo1T4z9
cTja3W61RZM6d07800kgZeN8rQPvTIDumMrgZK5D7ozNMWels3DbLJ1wYu4GMPBDefu8g0qfpQv8GeU
oEMVtFRfd1/TC8/51R9U42v4+wKpAAMqmFhvUoy3FqouzIqk+fY1sax7gT5MnuFF/sy5RND/+Zetr2+S
mvxYNBZ0gjo2dLzL/IFiz9NrIrYbNYgCBqXqmDwokAigxyd/BEPFGXuhRmS5T9LHKaLYaZs= daniel@
Daniels-MacBook-Pro.local
volt% █
```

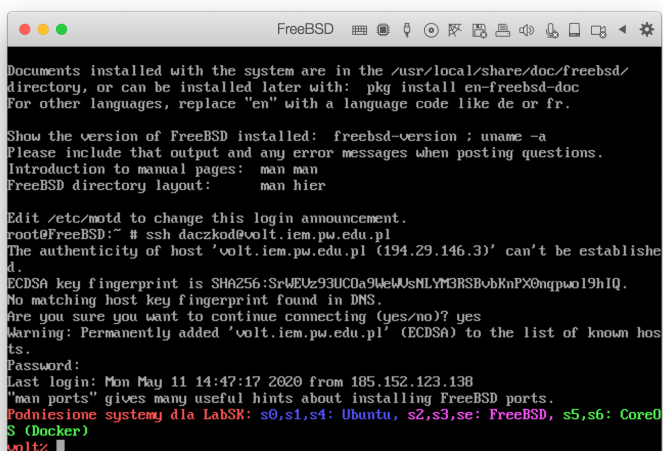
## 2.2 Kreacja maszyny wirtualnej FreeBSD 64-bit

### 2.2.1 Pobranie obrazu systemu i instalacja

W celu zainstalowania systemu FreeBSD na maszynie wirtualnej w środowisku *Parallels Desktop* rozpocząłem pobieraniu obrazu systemu:

```
[daniel@Daniels-MacBook-Pro ~ % curl -LRO http://zet.pw.edu.pl/pub/FreeBSD/zetis/]
freebsd-mfs-13.0-CURRENT-amd64.iso
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
1 224M 1 2544k 0 0 431k 0 0:08:53 0:00:05 0:08:48 451k█
```

Następnie przy pomocy interfejsu użytkownika programu *Parallels Desktop* utworzyłem maszynę wirtualną, przypisałem jej pamięć RAM o wielkości 2048MB i jako źródło sieci wybrałem sieć mostkowaną. W celu sprawdzenia poprawności działania w sieci podjąłem próbę połączenia się poprzez SSH z serwerem VOLT:



```
Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with: pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages: man man
FreeBSD directory layout: man hier

Edit /etc/motd to change this login announcement.
root@FreeBSD:~ # ssh daczkod@volt.iem.pw.edu.pl
The authenticity of host 'volt.iem.pw.edu.pl (194.29.146.3)' can't be established.
ECDSA key fingerprint is SHA256:SrWEUz93UC0a9WeWUsNLYM3RBSBvbkKnFX0ngpwo19hIQ.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'volt.iem.pw.edu.pl' (ECDSA) to the list of known hos
ts.
Password:
Last login: Mon May 11 14:47:17 2020 from 185.152.123.138
"man ports" gives many useful hints about installing FreeBSD ports.
Podniesione systemy dla LabSK: s0,s1,s4: Ubuntu, s2,s3,s6: FreeBSD, s5,s6: Core0
S (Docker)
volt% █
```

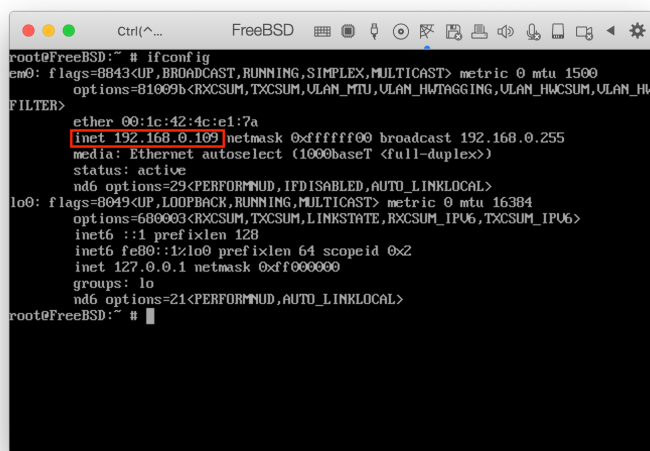
## 2.2.2 Sprawdzenie dwóch wariantów konfiguracji sieci maszyny wirtualnej

- Mostek (Bridge)

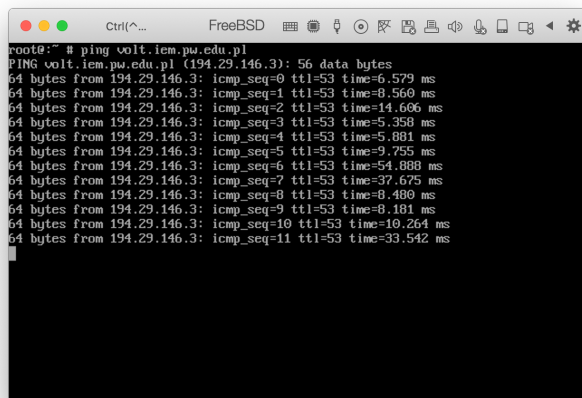
Ponieważ maszyna wirtualna była stworzona od razu w tym wariancie, od razu mogłem sprawdzić działanie sieci. W rezultacie:

- Maszyna wirtualna pojawia się jako osobny komputer należący do tej samej podsieci, co komputer Mac, na którym jest uruchomiona.
- Serwer DHCP (np. trasownik) zapewnia maszynie wirtualnej adres IP w tym samym zakresie IP, co inne komputery w tej samej podsieci.
- Maszyna wirtualna może pingować i wyświetlać wszystkie komputery w podsieci.
- Inne komputery mogą pingować i widzieć maszynę wirtualną.

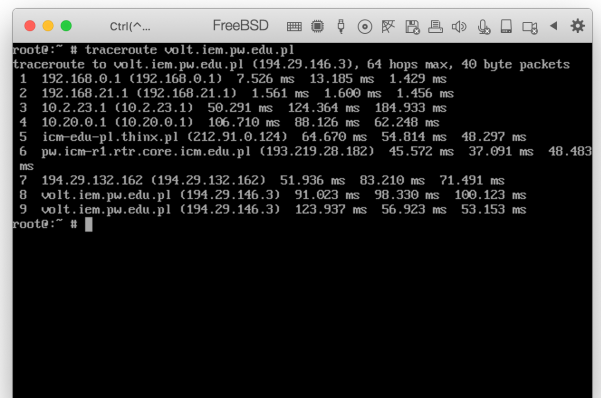
Sprawdziłem działanie przy pomocy poleceń `ifconfig`, `ping` i `traceroute`:



```
root@FreeBSD:~ # ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=81009b<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,ULAN_HWCSUM,ULAN_HWTAGGING>
    ether 00:1c:42:4c:e1:7a
    inet 192.168.0.109 netmask 0xfffff00 broadcast 192.168.0.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
    inet 127.0.0.1 netmask 0xff000000
    groups: lo
    nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
root@FreeBSD:~ #
```



```
root@:~ # ping volt.icm.pw.edu.pl
PING volt.icm.pw.edu.pl (194.29.146.3): 56 data bytes
64 bytes from 194.29.146.3: icmp_seq=0 ttl=53 time=6.579 ms
64 bytes from 194.29.146.3: icmp_seq=1 ttl=53 time=8.560 ms
64 bytes from 194.29.146.3: icmp_seq=2 ttl=53 time=14.606 ms
64 bytes from 194.29.146.3: icmp_seq=3 ttl=53 time=5.358 ms
64 bytes from 194.29.146.3: icmp_seq=4 ttl=53 time=5.881 ms
64 bytes from 194.29.146.3: icmp_seq=5 ttl=53 time=9.755 ms
64 bytes from 194.29.146.3: icmp_seq=6 ttl=53 time=54.888 ms
64 bytes from 194.29.146.3: icmp_seq=7 ttl=53 time=37.675 ms
64 bytes from 194.29.146.3: icmp_seq=8 ttl=53 time=8.480 ms
64 bytes from 194.29.146.3: icmp_seq=9 ttl=53 time=8.181 ms
64 bytes from 194.29.146.3: icmp_seq=10 ttl=53 time=10.264 ms
64 bytes from 194.29.146.3: icmp_seq=11 ttl=53 time=33.542 ms
root@:~ #
```



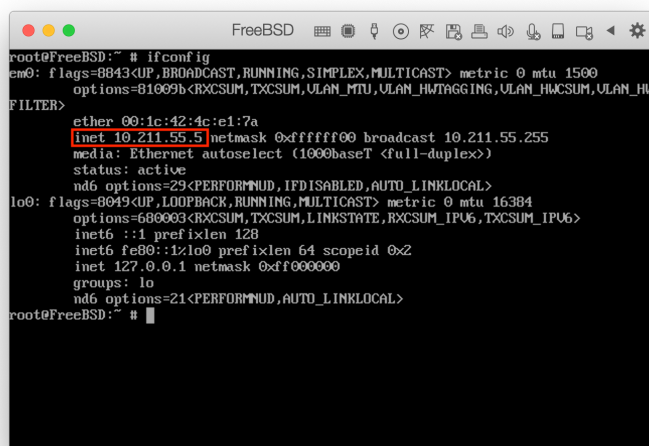
```
root@:~ # traceroute volt.icm.pw.edu.pl
traceroute to volt.icm.pw.edu.pl (194.29.146.3), 64 hops max, 40 byte packets
 1 192.168.0.1 (192.168.0.1) 7.526 ms 13.185 ms 1.429 ms
 2 192.168.21.1 (192.168.21.1) 1.561 ms 1.600 ms 1.456 ms
 3 10.2.23.1 (10.2.23.1) 50.291 ms 124.364 ms 184.933 ms
 4 10.20.0.1 (10.20.0.1) 106.710 ms 88.126 ms 62.248 ms
 5 icm-edu-pl.thinx.pl (212.91.0.124) 64.670 ms 54.814 ms 48.297 ms
 6 pw.icm-r1.rtr.core.icm.edu.pl (193.219.28.182) 45.572 ms 37.091 ms 48.483 ms
 7 194.29.132.162 (194.29.132.162) 51.936 ms 83.210 ms 71.491 ms
 8 volt.icm.pw.edu.pl (194.29.146.3) 91.023 ms 98.330 ms 100.123 ms
 9 volt.icm.pw.edu.pl (194.29.146.3) 123.937 ms 56.923 ms 53.153 ms
root@:~ #
```

- Translator adresów (NAT)

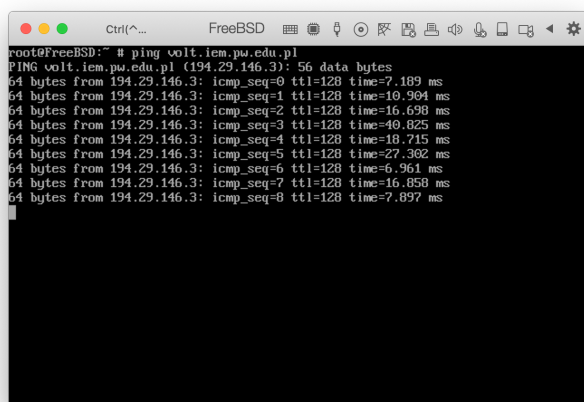
Zmieniłem w ustawieniach maszyny wirtualnej wariant sieci na opcję NAT. W rezultacie:

- *Parallels Desktop* tworzy oddzielną, wirtualną podsieć z własnym wirtualnym serwerem DHCP działającym w systemie macOS.
- Maszyna wirtualna należy do tej wirtualnej podsieci z własnym zakresem adresów IP.
- Maszyna wirtualna nie jest widoczna w prawdziwej podsieci, do której należy komputer Mac.
- Maszyna wirtualna korzysta z pełnego dostępu do Internetu.

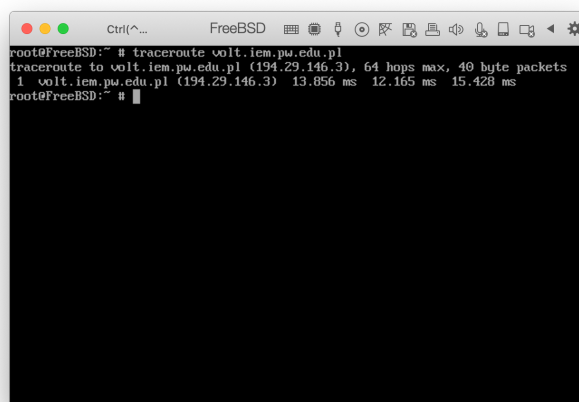
Ponownie skorzystałem z poleceń `ifconfig`, `ping` i `traceroute`:



```
root@FreeBSD:~ # ifconfig
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
    options=81009b<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,ULAN_HWCSUM,ULAN_HWTAGGING>
    ether 00:1c:42:4c:e1:7a
    inet 10.211.55.5 netmask 0xfffff00 broadcast 10.211.55.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMMUD,IFDISABLED,AUTO_LINKLOCAL>
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
    options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
    inet 127.0.0.1 netmask 0xff000000
    groups: lo
    nd6 options=21<PERFORMMUD,AUTO_LINKLOCAL>
root@FreeBSD:~ #
```



```
root@FreeBSD:~ # ping volt.icm.pw.edu.pl
PING volt.icm.pw.edu.pl (194.29.146.3): 56 data bytes
64 bytes from 194.29.146.3: icmp_seq=0 ttl=128 time=7.189 ms
64 bytes from 194.29.146.3: icmp_seq=1 ttl=128 time=10.904 ms
64 bytes from 194.29.146.3: icmp_seq=2 ttl=128 time=16.698 ms
64 bytes from 194.29.146.3: icmp_seq=3 ttl=128 time=40.825 ms
64 bytes from 194.29.146.3: icmp_seq=4 ttl=128 time=18.715 ms
64 bytes from 194.29.146.3: icmp_seq=5 ttl=128 time=27.302 ms
64 bytes from 194.29.146.3: icmp_seq=6 ttl=128 time=16.961 ms
64 bytes from 194.29.146.3: icmp_seq=7 ttl=128 time=16.858 ms
64 bytes from 194.29.146.3: icmp_seq=8 ttl=128 time=7.897 ms
root@FreeBSD:~ #
```



```
root@FreeBSD:~ # traceroute volt.icm.pw.edu.pl
traceroute to volt.icm.pw.edu.pl (194.29.146.3), 64 hops max, 40 byte packets
 1 volt.icm.pw.edu.pl (194.29.146.3) 13.856 ms 12.165 ms 15.428 ms
root@FreeBSD:~ #
```

### 3 Podsumowanie i wnioski

Ćwiczenie przebiegło pomyślnie. Udało mi się zrealizować wszystkie postawione zadania. Dla różnych wariantów sieci maszyny wirtualnej otrzymaliśmy różne adresy IP, co jest zgodne z moimi oczekiwaniami. Ruch `traceroute` może być blokowany przez niektóre zapory, jeśli włączoną mamy opcję NAT, dlatego też zauważamy różnice w jego działaniu dla różnych wariantów konfiguracji.