

Sprawozdanie z pracowni specjalistycznej

Bezpieczeństwo Sieci Komputerowych

Ćwiczenie numer: 2

Temat: *Serwer SSH*

Wykonujący ćwiczenie:

Paweł Orzel

Łukasz Hossa

Kacper Seweryn

Studia dzienne

Kierunek: Informatyka

Semestr: VI

Grupa zajęciowa: Grupa PS 10

Prowadzący ćwiczenie: mgr inż. Katarzyna Borowska

Data wykonania ćwiczenia: 07.03.2022

1. Teoria

SSH jest to protokół komunikacyjny stosowany w sieciach TCP/IP. Służy do zdalnego łączenia terminalowego z komputerami. SSH jest następcą protokołu telnet - w przeciwieństwie do swojego poprzednika, połączenia zestawiane przez SSH są szyfrowane.

Na bazie SSH powstało kilka bezpiecznych protokołów transferu plików np. SCP i SFTP. Protokół SSH, działa w architekturze klient-serwer i jego usługa nasłuchuje na domyślnym porcie 22. Najpopularniejszy zestaw narzędzi do zarządzania SSH, to pakiet OpenSSH zainstalowany domyślnie w większości dystrybucji GNU/Linux i BSD. OpenSSH standardowo zawiera serwer SSH oraz klienta SSH.

2. Realizacja zadania

2.1. Instalacja serwera oraz narzędzia nmap

Instalacja niezbędnych programów potrzebnych do realizacji zadania.

```
student@student-VirtualBox:~$ sudo apt-get install openssh-server nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-38-generic linux-hwe-5.11-headers-5.11.0-38
  linux-image-5.11.0-38-generic linux-modules-5.11.0-38-generic
  linux-modules-extra-5.11.0-38-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libblas3 liblinear4 lua-lpeg ncurses-term nmap-common openssh-client
  openssh-sftp-server ssh-import-id
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap keychain libpam-ssh
  monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  libblas3 liblinear4 lua-lpeg ncurses-term nmap nmap-common openssh-server
  openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 9 newly installed, 0 to remove and 64 not upgraded.
Need to get 6 912 kB of archives.
After this operation, 32,3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://pl.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-client
amd64 1:8.2p1-4ubuntu0.4 [671 kB]
Get:2 http://pl.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0-1b
```

2.2 Sprawdź status usługi

```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Mon 2022-03-07 10:29:30 CET; 15s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 3474 (sshd)
    Tasks: 1 (limit: 9464)
   Memory: 1.0M
   CGroup: /system.slice/ssh.service
           └─3474 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

Usługa działa poprawnie o czym świadczy napis active.

2.3* Sprawdź z innego urządzenia, czy połączenia z serwerem SSH są dozwolone- zadanie dodatkowe: sprawdź z poziomu urządzenia klienta, jakie porty są otwarte na serwerze. Na liście powinien być serwer SSH.

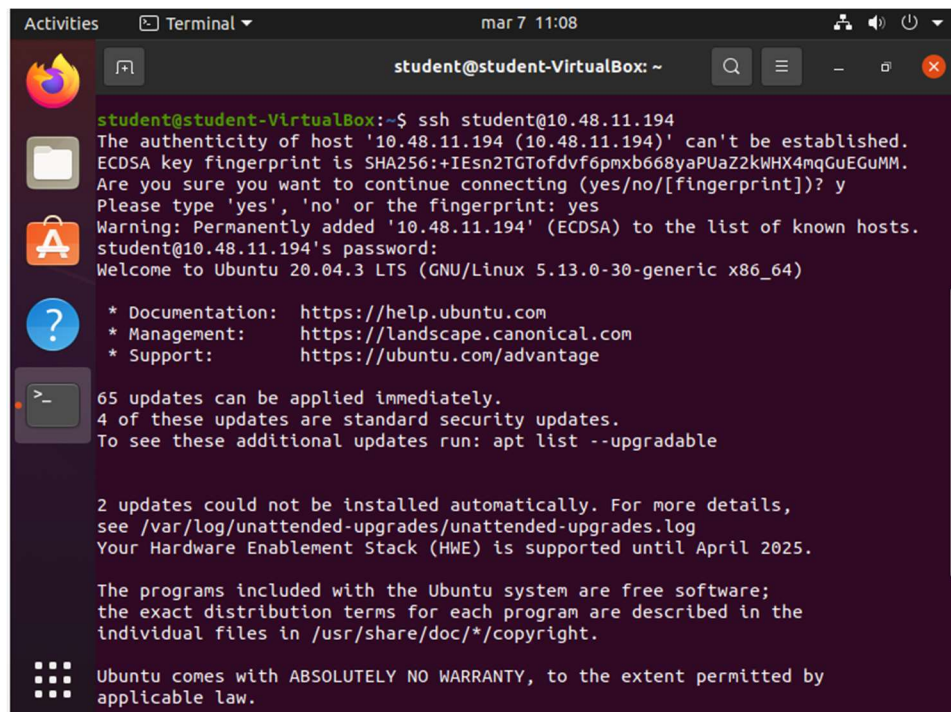
Za pomocą nmap sprawdzamy jakie porty są dostępne, w naszym przypadku port 22

```
student@student-VirtualBox:~$ sudo nmap 10.48.11.194
[sudo] password for student:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 11:06 CET
Nmap scan report for student-VirtualBox (10.48.11.194)
Host is up (0.0000020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

2.3 Sprawdź z innego urządzenia, czy połączenia z serwerem SSH są dozwolone.

Po wprowadzeniu odpowiedniego adresu powinniśmy móc się połączyć z serwerem ssh



```
student@student-VirtualBox:~$ ssh student@10.48.11.194
The authenticity of host '10.48.11.194 (10.48.11.194)' can't be established.
ECDSA key fingerprint is SHA256:+IEsn2GTofdvf6pmxb668yaPUaZ2kWHX4mqGuEGuMM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.48.11.194' (ECDSA) to the list of known hosts.
student@10.48.11.194's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

65 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

2.4 Zmodyfikuj plik konfiguracyjny serwera (/etc/ssh/sshd_config) tak, aby serwer działał na porcie 10022. Zrestartuj serwer i połącz się z nim.

```
student@student-VirtualBox: /etc/ssh
GNU nano 4.8          sshd_config          Modifiec

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 10022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

2.4 Restart na nowym porcie(na górze dyrektywa Port była odkomentowana)

```
student@student-VirtualBox:/etc/ssh$ service ssh restart
student@student-VirtualBox:/etc/ssh$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Mon 2022-03-07 11:09:25 CET; 4s ago
```

2.4*. Sprawdź jakie otwarte porty są wypisywane przez polecenie nmap, gdy jest uruchomione z domyślnymi opcjami (tak jak poprzednio). Czy ten port jest wypisywany?

```
Activities  Terminal  mar 7 11:13
student@student-VirtualBox: ~

student@student-VirtualBox:~$ ssh student@10.48.11.194 -p 10022
student@10.48.11.194's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

65 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar  7 11:10:08 2022 from 82.139.145.216
student@student-VirtualBox:~$ sudo nmap 10.48.11.194
[sudo] password for student:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 11:11 CET
Nmap scan report for student-VirtualBox (10.48.11.194)
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
student@student-VirtualBox:~$
```

Port 10022 **nie jest** wypisywany. Dzieje się tak, ponieważ nmap nie widzi niestandardowych portów i ich nie analizuje.

2.4 Zmiana portu na domyślny


```

ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e
Active: active (running) since Mon 2022-03-07 11:13:44 CET; 5s ago
Docs: man:sshd(8)
      man:sshd_config(5)
Process: 2934 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 2935 (sshd)
Tasks: 1 (limit: 9464)
Memory: 1.0M
CGroup: /system.slice/ssh.service
        └─2935 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

mar 07 11:13:44 student-VirtualBox systemd[1]: Starting OpenBSD Secure Shell se
mar 07 11:13:44 student-VirtualBox sshd[2935]: Server listening on 0.0.0.0 port
mar 07 11:13:44 student-VirtualBox sshd[2935]: Server listening on :: port 22.

```

2.5 W pliku konfiguracyjnym serwera ustaw dyrektywę:

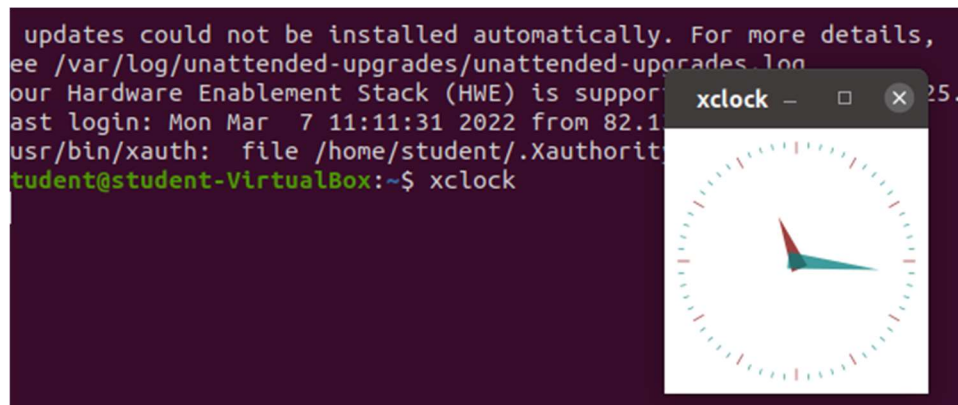
X11Forwarding yes

Sprawdź, czy rzeczywiście protokół X11 jest forwardowany uruchamiając w sesji SSH wybraną aplikację z interfejsem graficznym, np. xclock, firefox, etc. Pamiętaj o użyciu klucza **-X** podczas nawiązywania połączenia.

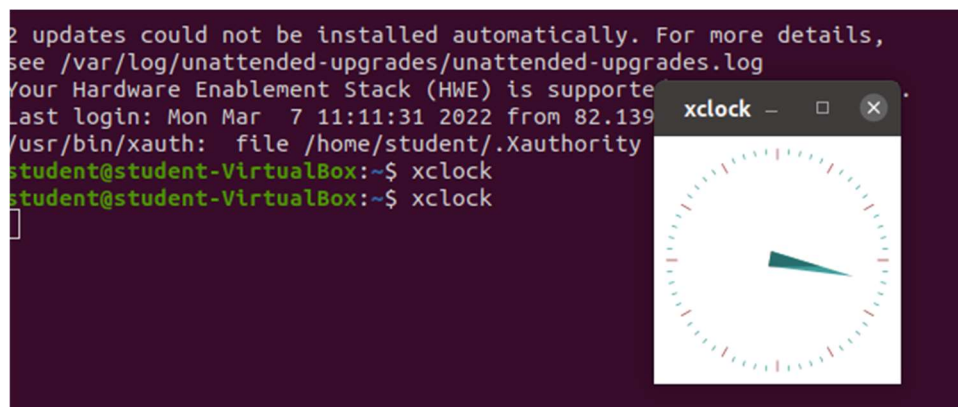
Godzina na serwerze

mar 7 03:17

2.5 Xclock – przed zmianą godziny



2.5 Xclock – zmiana godziny



Powyżej widać poprawne działanie forwardowania protokołu X11.

2.6. Powtórz poprzednie zadanie, ale z zablokowanym forwardowaniem protokołu X11.

X11Forwarding no

```
X11Forwarding no
```

2.6 Xclock-blokada

```
2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar  7 03:15:26 2022 from 82.139.145.216
student@student-VirtualBox:~$ xclock
Error: Can't open display:
student@student-VirtualBox:~$
```

Tym razem przy braku forwardowania nie mamy dostępu do zegara.

2.7 Sprawdź zachowanie klienta w przypadku, gdy fingerprint serwera uległ zmianie.

2.7 Usunięcie kluczy

Usuwanie w ten sposób klucze publiczne użytkowników, którzy weszli już na serwer

```
sudo rm /etc/ssh/ssh_host_*_key
```

2.7 Wygenerowanie nowych kluczy

```
student@student-VirtualBox:/etc/ssh$ sudo ssh-keygen -A
ssh-keygen: generating new host keys: RSA DSA ECDSA ED25519
```

2.7 Prośba o połączenie po zmianie kluczy

```
Connection to 10.48.11.194 closed.
student@student-VirtualBox:~$ ssh student@10.48.11.194
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:KkAL8+B3joErXRVJ+9HctX5YaNqtXjwF+++FNcdwGIE.
Please contact your system administrator.
Add correct host key in /home/student/.ssh/known_hosts to get rid of this messa
ge.
Offending ECDSA key in /home/student/.ssh/known_hosts:1
  remove with:
  ssh-keygen -f "/home/student/.ssh/known_hosts" -R "10.48.11.194"
ECDSA host key for 10.48.11.194 has changed and you have requested strict check
ing.
Host key verification failed.
student@student-VirtualBox:~$
```

W przypadku usunięcia kluczy publicznych użytkowników i wygenerowania nowych, użytkownik nie będzie miał dostępu do serwera, dopóki nie usunie u siebie starych kluczy i nie pobierze nowych z serwera.

2.8. Skonfiguruj dostęp do konta np. lpic na serwerze SSH z dostępem poprzez klucz, zamiast hasła.

```

student@student-VirtualBox:~$ ssh-keygen -f "/home/student/.ssh/known_hosts" -R
"10.48.11.194"
# Host 10.48.11.194 found: line 1
/home/student/.ssh/known_hosts updated.
Original contents retained as /home/student/.ssh/known_hosts.old
student@student-VirtualBox:~$ ssh student@10.48.11.194
The authenticity of host '10.48.11.194 (10.48.11.194)' can't be established.
ECDSA key fingerprint is SHA256:KkAL8+B3joErXRVJ+9HctX5YaNqtXjwF+++FNcdwGIE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.11.194' (ECDSA) to the list of known hosts.
student@10.48.11.194's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

65 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar  7 03:18:16 2022 from 82.139.145.216

```

2.8 Przesłanie klucza publicznego

Naszym użytkownikiem jest lpic2

```

student@student-VirtualBox:~$ ssh-copy-id lpic2@10.48.11.194
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
lpic2@10.48.11.194's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'lpic2@10.48.11.194'"
and check to make sure that only the key(s) you wanted were added.

```

2.8 Zalogowanie na nowego usera

```

student@student-VirtualBox:~$ ssh lpic2@10.48.11.194
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

65 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
lpic2@student-VirtualBox:~$

```

Połączenie z poziomu użytkownika student na serwerowe konto lpic2 przebiegło pomyślnie.

2.9 Korzystanie z serwera SFTP.

Upewnij się, że pliku konfiguracyjnym serwera (/etc/ssh/sshd_config) odblokowana jest dyrektywa:

override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

```
# override default of no subsystems
Subsystem      sftp      /usr/lib/openssh/sftp-server
```

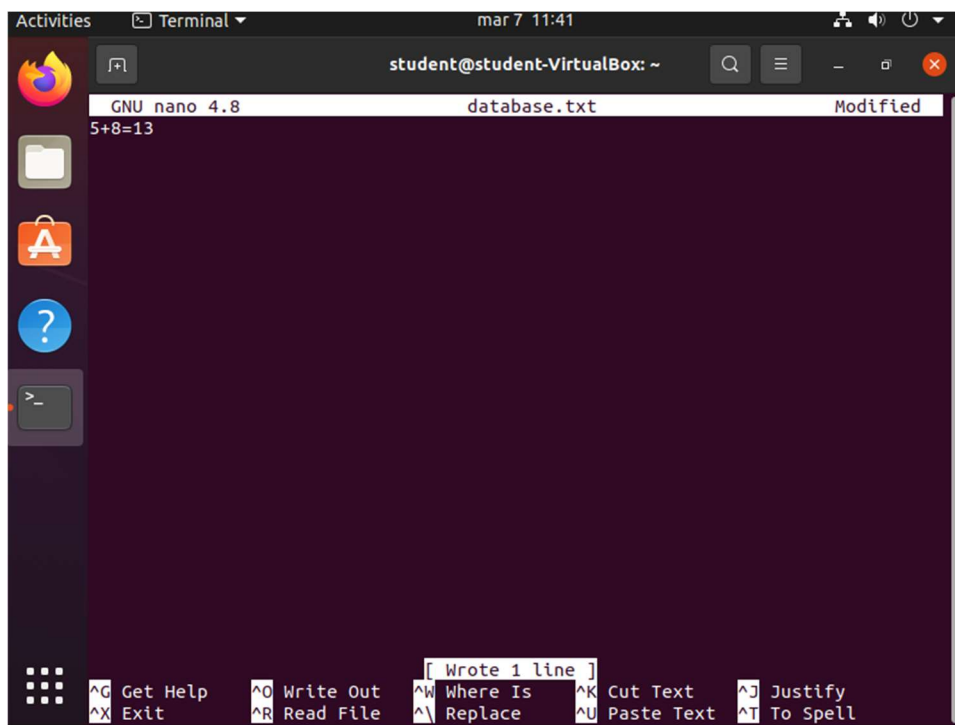
2.9 Utwórz na urządzeniu lokalnym plik do nazwie **database.txt**, którym zapisane jest dowolne zadanie matematyczne, np. "5+7".

```
student@student-VirtualBox:~$ sudo echo "5+7" > database.txt
```

2.9 Następnie skopiuj go pod zmienioną nazwą **math.txt** do katalogu domowego użytkownika **student** na serwerze SSH:

```
student@student-VirtualBox:~$ scp database.txt student@10.48.11.194:math.txt
student@10.48.11.194's password:
database.txt                                100%   4    21.2KB/s   00:00
```

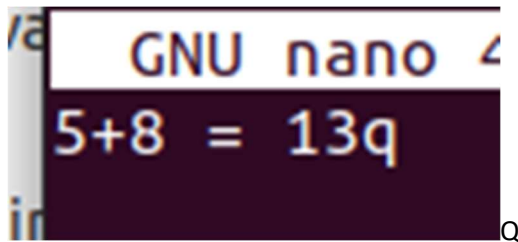
W naszym przypadku edytowaliśmy treść pliku txt, aby treść była unikatowa dla naszej grupy



2.9 Ustawienie z urządzenia lokalnego

```
5+8 = 13q
```

2.9 Wygląd po stronie serwera



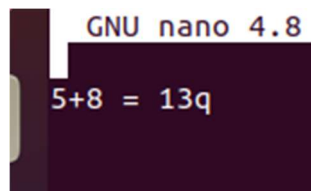
2.9 Lokalnie zapisany plik mathq.txt

```

Connection to 10.48.11.194 closed.
student@student-VirtualBox:~$ ls
cron.sh      Downloads  Music      program1.c  Public    T
database.txt funkcja.c  Pictures   program1.o  q         Templates
Desktop      main.c     program    program.c   q.pub     Videos
Documents    math.txt   program1   program.o   snap      wypisz
student@student-VirtualBox:~$ nano math.txt
student@student-VirtualBox:~$ qqqqqqqq

```

2.9 Zawartość math.txt lokalnie



Zmiany zachodzące w pliku były widoczne zarówno po stronie klienta jak i serwera. Klient pobrał rozwiązane zadanie z poziomu użytkownika serwerowego, co potwierdza poprawne działanie serwera SFTP.

3. Wnioski

Udało się zrealizować poprawnie wszystkie zadania. Zapoznaliśmy się z podstawową obsługą serwera SSH. Plik konfiguracyjny serwera znajduje się pod ścieżką: **/etc/ssh/sshd_config**, odpowiednio konfiguruując ten plik możemy zmieniać port serwera. Forwardowanie protokołu X11 pozwoliło na przedstawienie zmian zachodzących na serwerze z poziomu klienta za pomocą graficznego zegara analogowego. Podczas pierwszego logowania użytkownika na serwer tworzony jest klucz użytkownika, który jest sprawdzany podczas próby ponownego zalogowania. Możemy generować nowe klucze na serwerze oraz je usuwać. Za pomocą SFTP został zrealizowany ostatni podpunkt zadania, który polegał na wymianie plików między serwerem a klientem. Protokół umożliwił dla klienta skopiowanie danego pliku z serwera.sft