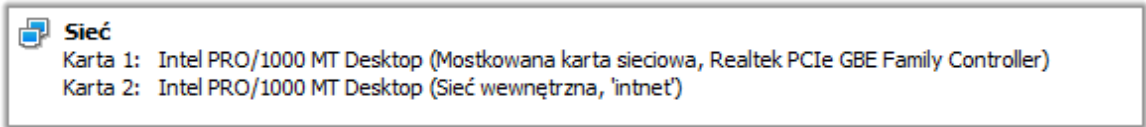


Serwer SSH

1. Na maszynie z US przywracamy czystą migawkę (może być ta z konfiguracji kart sieciowych), **pierwszą sieć** konfigurujemy jako **zmostkowaną**, **drugą** jako **wewnętrzną intnet** (tak jak w poprzednim ćwiczeniu)



2. Przygotowujemy sobie jakąś drugą maszynę na testy (7,10, XP) sieć **wewnętrzna intnet**
3. Uruchamiamy Ubuntu, konfigurujemy kartę sieciową (tak aby adresacja pasowała do naszej sieci domowej) i **końcówka adresu IP** to był **nasz numer z dziennika**. Druga sieć to 192.168.X.1/24. U mnie niech to będzie:

pierwsza sieć

IP:10.39.100.X

M:255.0.0.0

B:10.0.0.1

DNS:8.8.8.8

druga sieć:

IP:192.168.X.1

M:255.255.255.0

cd /etc/netplan/

nano 01-netcf.yaml

modyfikujemy ustawienia

netplan apply

```
GNU nano 2.9.3 /etc/netplan/01-netcf.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [192.168.1.200/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
    enp0s8:
      dhcp4: false
      addresses: [10.0.0.1/8]

[ Read 18 lines ]
^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit          ^R Read File    ^_ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

4. Uaktualniamy listę zawartości repozytoriów przed instalacją serwera SSH (od Ubuntu 16.04 w górę możemy używać `apt update` zamiast `apt-get update`, tak samo przy instalacji wystarczy `apt install` zamiast `apt-get install`)

apt update

```
root@jkubuntu:/etc/netplan# apt update
Stary:1 http://pl.archive.ubuntu.com/ubuntu bionic InRelease
Stary:2 http://pl.archive.ubuntu.com/ubuntu bionic-updates InRelease
Stary:3 http://pl.archive.ubuntu.com/ubuntu bionic-backports InRelease
Stary:4 http://pl.archive.ubuntu.com/ubuntu bionic-security InRelease
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
38 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@jkubuntu:/etc/netplan#
```

5. Instalujemy serwer ssh - użyjemy pakietu **openssh-server**

apt install openssh-server

```

ntu1.18.04 [248 kB]
Pobieranie:3 http://p1.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sftp-server amd64
1:7.6p1-4ubuntu0.3 [45,6 kB]
Pobieranie:4 http://p1.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-server amd64 1:7.
6p1-4ubuntu0.3 [333 kB]
Pobieranie:5 http://p1.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-id all 5.7-0ub
untu1.1 [10,9 kB]
Pobrano 683 kB w 0s (14578 kB/s)
Prekonfiguracja pakietów ...
Wybieranie wcześniej niewybranego pakietu libwrap0:amd64.
(Odczytywanie bazy danych ... 99682 pliki i katalogi obecnie zainstalowane.)
Przygotowywanie do rozpakowania pakietu ../libwrap0_7.6.q-27_amd64.deb ...
Rozpakowywanie pakietu libwrap0:amd64 (7.6.q-27) ...
Wybieranie wcześniej niewybranego pakietu ncurses-term.
Przygotowywanie do rozpakowania pakietu ../ncurses-term_6.1-1ubuntu1.18.04_all.deb ...
Rozpakowywanie pakietu ncurses-term (6.1-1ubuntu1.18.04) ...
Wybieranie wcześniej niewybranego pakietu openssh-sftp-server.
Przygotowywanie do rozpakowania pakietu ../openssh-sftp-server_1%3a7.6p1-4ubuntu0.3_amd64.deb ...
Rozpakowywanie pakietu openssh-sftp-server (1:7.6p1-4ubuntu0.3) ...
Wybieranie wcześniej niewybranego pakietu openssh-server.
Przygotowywanie do rozpakowania pakietu ../openssh-server_1%3a7.6p1-4ubuntu0.3_amd64.deb ...
Rozpakowywanie pakietu openssh-server (1:7.6p1-4ubuntu0.3) ...
Wybieranie wcześniej niewybranego pakietu ssh-import-id.
Przygotowywanie do rozpakowania pakietu ../ssh-import-id_5.7-0ubuntu1.1_all.deb ...
Rozpakowywanie pakietu ssh-import-id (5.7-0ubuntu1.1) ...
Konfigurowanie pakietu ncurses-term (6.1-1ubuntu1.18.04) ...
Konfigurowanie pakietu openssh-sftp-server (1:7.6p1-4ubuntu0.3) ...
Konfigurowanie pakietu ssh-import-id (5.7-0ubuntu1.1) ...
Konfigurowanie pakietu libwrap0:amd64 (7.6.q-27) ...
Konfigurowanie pakietu openssh-server (1:7.6p1-4ubuntu0.3) ...

Creating config file /etc/ssh/sshd_config with new version
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.se
rvice.

Progress: [ 92%] [#####.....]

```

(jak widzimy, polecenie apt install pokazuje nam pasek postępu instalacji)

6. Nasz serwer zaraz po instalacji powinien działać i pozwalać na podłączenie się na domyślnym 22 porcie. Możemy to sprawdzić przy pomocy polecenia:

service ssh status

lub

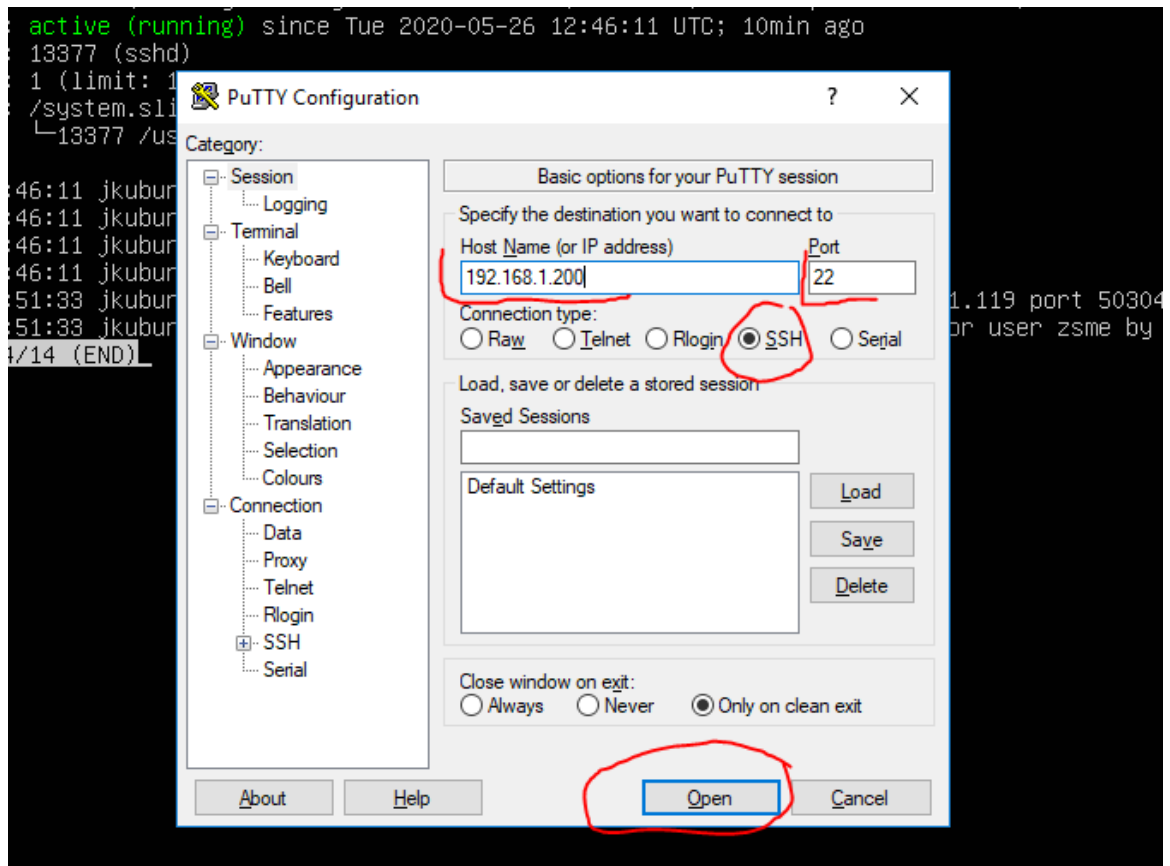
systemctl status ssh

(żeby wyjść z polecenia używamy Ctrl + C)

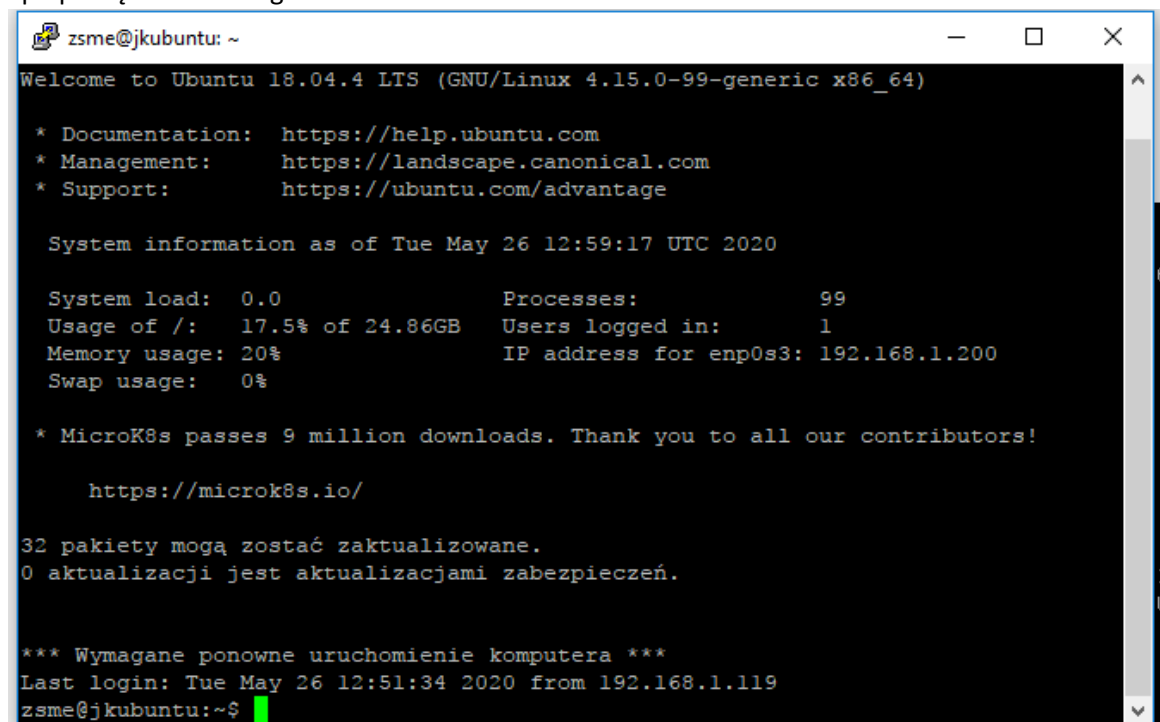
```
root@jkubuntu:/etc/ssh# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-05-26 12:46:11 UTC; 10min ago
 Main PID: 13377 (sshd)
    Tasks: 1 (limit: 1108)
   CGroup: /system.slice/ssh.service
           └─13377 /usr/sbin/sshd -D

maj 26 12:46:11 jkubuntu systemd[1]: Starting OpenBSD Secure Shell server...
maj 26 12:46:11 jkubuntu sshd[13377]: Server listening on 0.0.0.0 port 22.
maj 26 12:46:11 jkubuntu sshd[13377]: Server listening on :: port 22.
maj 26 12:46:11 jkubuntu systemd[1]: Started OpenBSD Secure Shell server.
maj 26 12:51:33 jkubuntu sshd[13592]: Accepted password for zsme from 192.168.1.119 port 50304 ssh2
maj 26 12:51:33 jkubuntu sshd[13592]: pam_unix(sshd:session): session opened for user zsme by (uid=0)
lines 1-14/14 (END)
```

7. Powinniśmy być się w stanie podłączyć na adres naszego serwera na domyślnym 22 porcie. Uruchamiamy Putty i zestawiamy połączenie:



i po podłączeniu i zalogowaniu:



8. Konfiguracja naszego serwera SSH znajduje się w katalogu `/etc/ssh` w pliku `sshd_config`

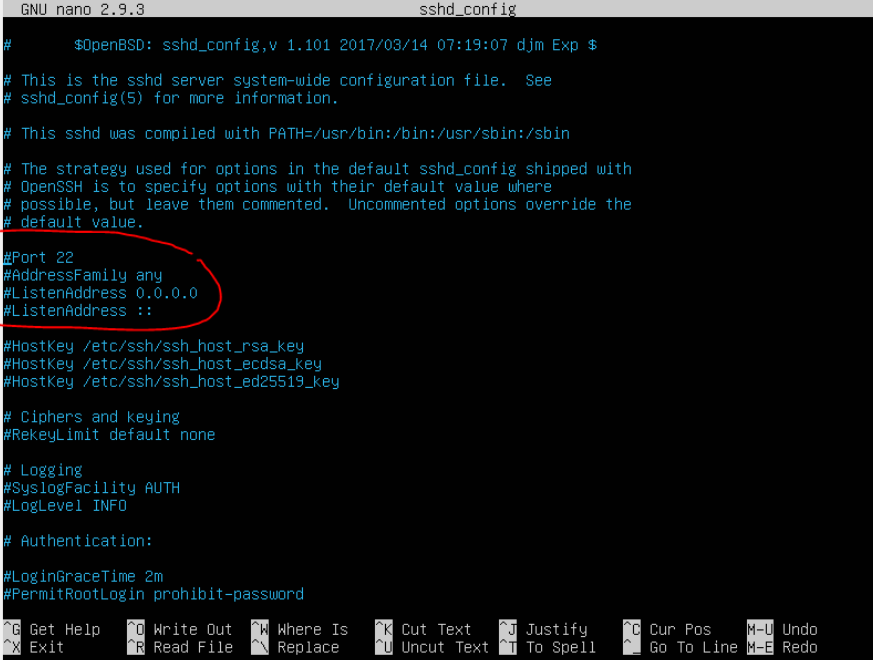
Przed zmianą konfiguracji zrobmy sobie oczywiście **kopie pliku konfiguracyjnego**, żeby w

razie wtopy można go było łatwo przywrócić:

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bac
```

otwieramy w edytorze plik konfiguracyjny

```
nano /etc/ssh/sshd_config
```



```
GNU nano 2.9.3 sshd_config
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# 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.
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password

G Get Help  O Write Out  W Where Is  K Cut Text  J Justify  C Cur Pos  M-U Undo
X Exit      R Read File  R Replace  U Uncut Text  T To Spell  G Go To Line M-B Redo
```

najczęściej będzie nasz interesowała opcja wybrania adresu na którym ma działać serwer oraz portu

Możemy dopisać dodatkowe porty na których ma nasłuchiwać nasz serwer, zmienić domyślny port - całość polega na odkomentowaniu odpowiedniej linijki i ewentualnie dopisania żądanych ustawień - założymy, że chcemy, żeby oprócz domyślnego portu serwer działał też na porcie 2222:

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# 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.

Port 22
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

[ Wrote 123 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
Use "fg" to return to nano.  ^R Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line  M-E Redo
```

oczywiście, żeby nasze zmiany miały skutek musimy zrestartować usługę poleceniem:

service ssh restart

lub

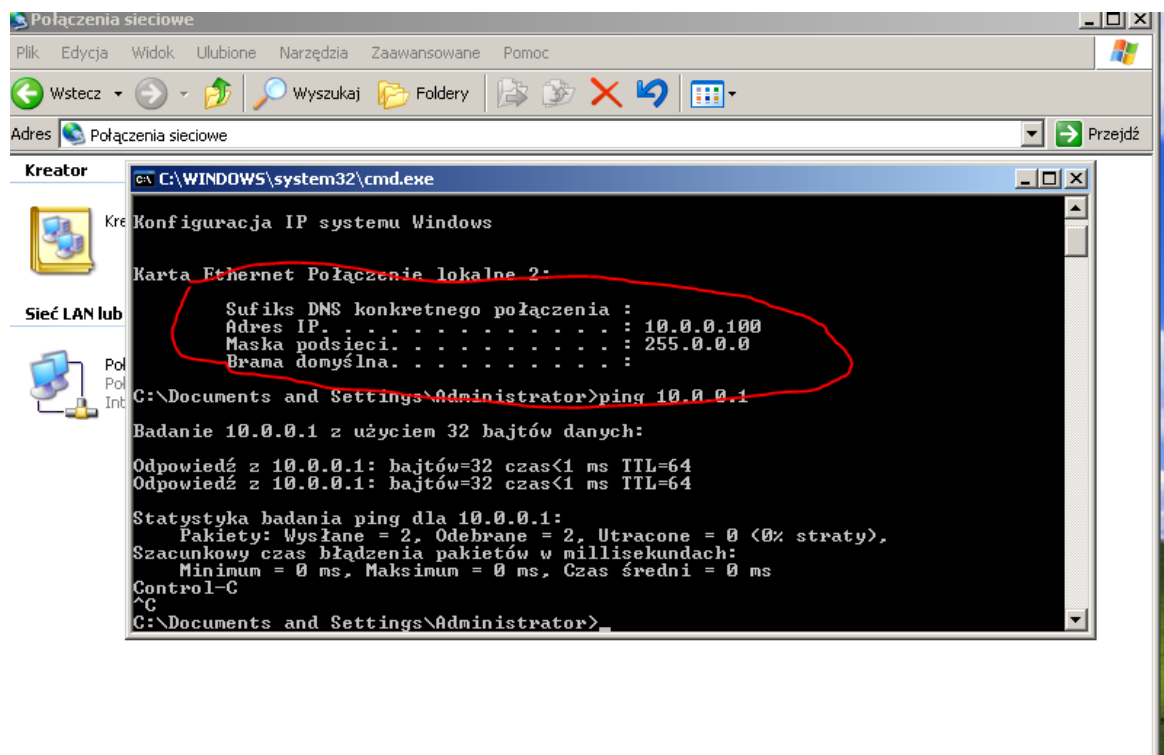
systemctl restart ssh

Serwer powinien pozwalać teraz na połączenia na porcie 22 i 2222

9. Przygotujmy sobie teraz maszynę testową - ja użyję Windowsa XP – najpierw uruchomię go z kartą sieciową zmostkowaną, żeby mieć internet, ściągnę Putty (32bity, bo to XP)



Po ściągnięciu Putty, zmieniamy typ sieciówki na wewnętrzną i ustawiamy adresację na pasującą do drugiej karty sieciowej na naszym serwerze, czyli na przykład 10.0.0.100/8



10. Możemy ustawić na jakim adresie/adresach IP ma nasłuchiwać nasz serwer – domyślnie nasłuchuje na wszystkich (powinien Was wpuścić i z komputera gospodarza i z komputera testowego na obu ustawionych portach) – odkomentowanie odpowiedniej linii i wpisanie adresu spowoduje, że serwer będzie nasłuchiwał tylko na jednym adresie:

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# 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.

Port 22
Port 2222
#AddressFamily any
ListenAddress 192.168.1.200
#ListenAddress ..

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

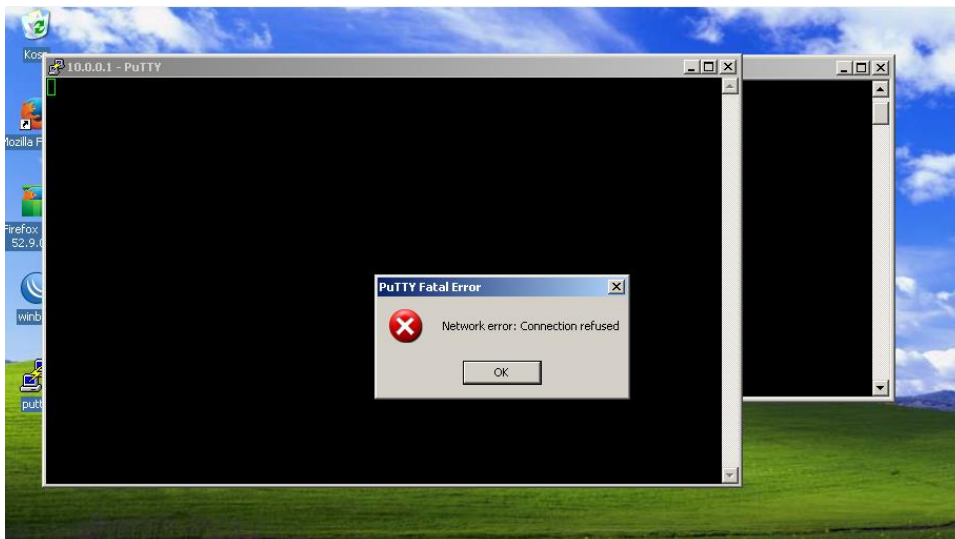
#LoginGraceTime 2m

[ Wrote 123 lines ]
Get Help Write Out Where Is Cut Text Justify Cur Pos M-U Undo
Use "fg" to return to nano. Replace U Uncut Text T To Spell Go To Line M-E Redo

[3]+ Stopped nano sshd_config
root@jkubuntu:/etc/ssh# systemctl restart ssh
root@jkubuntu:/etc/ssh# _
```

Oczywiście po zapisaniu restartujemy za każdym razem usługę ssh (service ssh restart)

Teraz próbując zalogować się z komputera testowego na adres 10.0.0.1 serwer powinien odrzucić połączenie:



11. Możemy ręcznie dopisać drugi adres w konfiguracji – tutaj dodatkowo podałem port 3333 – przy takiej notacji serwer będzie zezwalał na łączenie się na tym adresie tylko na porcie 3333 pomijając te ustawione wyżej:

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# 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.

Port 22
Port 2222
#AddressFamily any
ListenAddress 192.168.1.200
ListenAddress 10.0.0.1:3333
#ListenAddress :

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

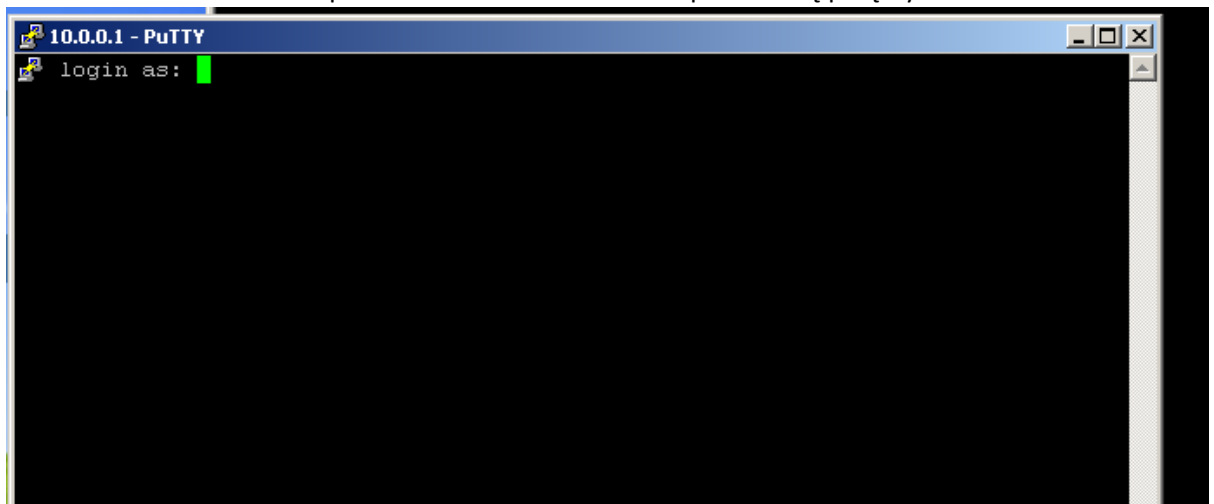
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify   ^G Cur Pos   M-U Undo
Use "fg" to return to nano.  ^\ Replace    ^U Uncut Text ^T To Spell  ^_ Go To Line  M-E Redo

[4]+  Stopped                  nano sshd_config
root@jkubuntu:/etc/ssh#
```

Oczywiście po restarcie usługi ssh i próbie połączenia się z komputera testowego na 10.0.0.1:22 serwer odrzuci połączenie a na 10.0.0.1:3333 pozwoli się połączyć.



12. Blokada lub zezwalanie na dostęp użytkowników/grup

Możemy też chcieć zablokować lub zezwalać na dostęp określonych użytkowników/grup

Musimy wtedy w naszym configu użyć odpowiednich zmiennych (działają zgodnie z nazwami):

```
DenyUsers user1 user2 user3
DenyGroups group1 group2
```

```
AllowUsers user1 user2
AllowGroups group1 group2
```

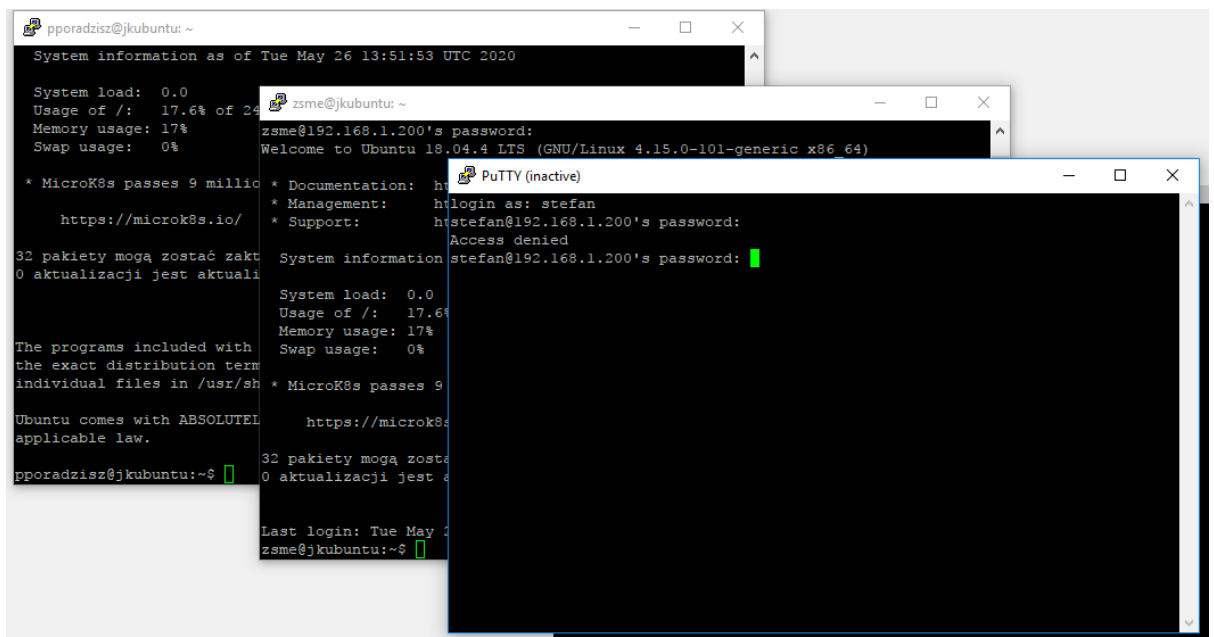
Załóżmy na serwerze testowe konto **inazwisko** z hasłem **123qwe** oraz **stefan** z hasłem **123qwe**

```
adduser pporadzisz
adduser stefan
```

I teraz spróbujemy ustawić tak, że konta inazwisko i zsmie są wpuszczane na serwer konto stefan nie:

```
GNU nano 2.9.3          sshd_config
#      $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
# 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.
Port 22
Port 2222
#AddressFamily any
ListenAddress 192.168.1.200
ListenAddress 10.0.0.1:3333
#ListenAddress :
DenyUsers stefan
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
```

restartujemy serwer SSH i sprawdzamy:



Podobnie oczywiście będzie działało to z grupami.