

Instalacja i konfiguracja serwera SSH.

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia, które użyjesz, aby:

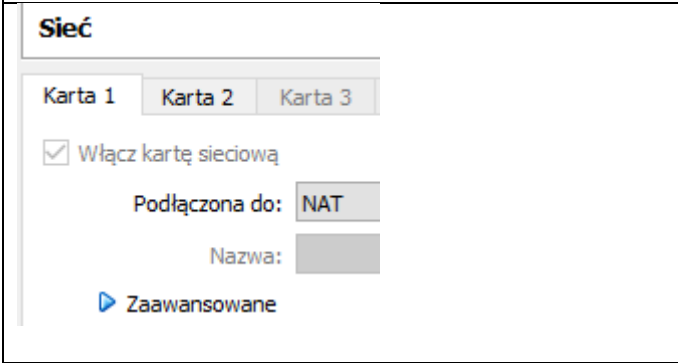
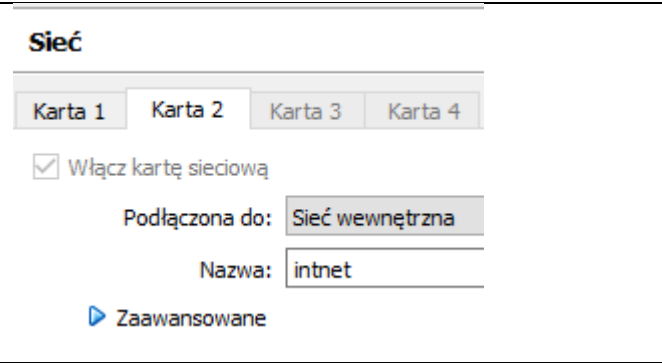
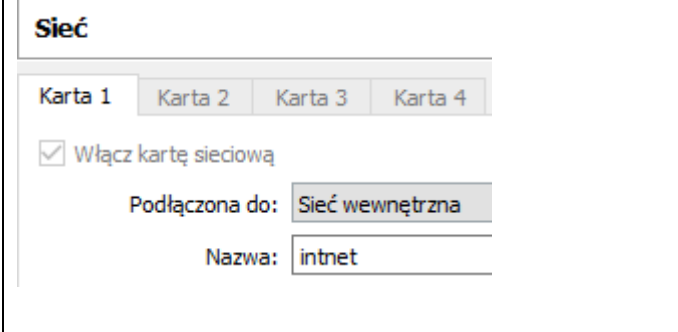
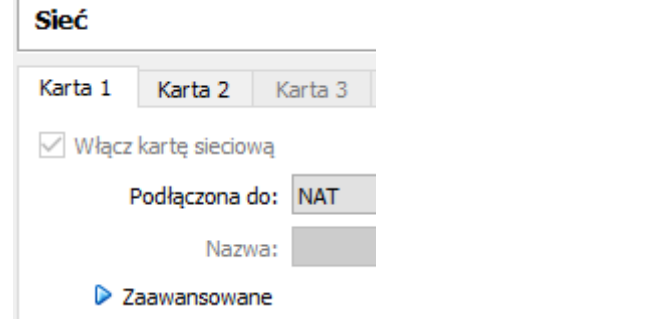
- wyjaśnić pojęcia związane z ssh,
- zainstalować serwer ssh,
- uruchomić lub zatrzymać usługi sieciowe,
- konfigurować serwer ssh,
- korzystać z ssh.

2. podaj odpowiedzi na pytania zadane w treści zadań.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Ubuntu serwer i klient. Przygotuj Ubuntu.

Do ćwiczenia potrzebna jest nowa (czysta) instalacja Windows. Przygotuj Windows.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu.

<p>Ubuntu serwer Adapter 1</p> 	<p>Ubuntu serwer Adapter 2</p> 
<p>Windows Adapter 1</p> 	<p>Ubuntu desktop Adapter 1</p> 

Po uruchomieniu Ubuntu podaj **login: ubuntu** **Password: ubuntu**

Wisz **sudo -s** **Password: ubuntu**

```
ubuntu@dlp:~$ sudo -s
[sudo] password for ubuntu:
```

Ustawienie statycznego adresu IP

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Za pomocą polecenia `ifconfig -a` ustal dostępne interfejsy sieciowe.

```
root@dlp:~# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe68:a08 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:68:0a:08 txqueuelen 1000 (Ethernet)
    RX packets 2712 bytes 2450820 (2.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1142 bytes 77401 (77.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

Plik `/etc/netplan/01-netcfg.yaml` - opisuje interfejsy sieciowe dostępne w systemie i jak je aktywować.

2. Zmień adres IP dla Ubuntu na enp0s8 (Adapter 2) na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe `nano /etc/netplan/0` tabulator `*.yaml`

Pozostaw zalecane wpisy w tym pliku

```
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s17:
      dhcp4: true
    enp0s8:
      dhcp4: no
      addresses: [10.0.0.30/24]
```

3. Zastosuj ustawienia

```
root@dlp:~# netplan apply
```

```
root@dlp:~# netplan apply
```

4. Wyświetl domyślną bramę (adres routera) dla interfejsów sieciowych serwera

```
root@dlp:~# ip route show default
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
```

Zapisz w zeszycie co się stało po wykonaniu poleceń. Wpisz kolejno polecenia.

Część 1 - Instalacja i konfiguracja serwera SSH dla Ubuntu serwer.

1. Wykonaj `root@dlp:~# apt -y install openssh-server`

Jeżeli nie jest możliwe zainstalowanie należy wykonać `apt-get update` - aktualizowanie listy pakietów, jeśli nie jest możliwe należy wykonać `apt-get upgrade` - aktualizacja systemu.

2. Kolejno zatrzymaj i uruchom usługę ssh

```
root@dlp:~# /etc/init.d/ssh stop
[ ok ] Stopping ssh (via systemctl): ssh.service.
root@dlp:~# /etc/init.d/ssh start
[ ok ] Starting ssh (via systemctl): ssh.service.
```

3. Zrestartuj usługę ssh

```
root@dlp:~# /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
```

4. Sprawdź poleceniem NETSTAT aktywne połączenia protokołu TCP, czy jest otwarty port 22 odpowiadający za ssh (port nasłuchujący ma otwarty = LISTEN)

```
root@dlp:~# netstat -ant | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp6       0      0 :::22             :::*                LISTEN
```

Jeśli nie jest to zainstaluj program nmap `root@dlp:~# apt install nmap`

5. Sprawdź czy usługa ssh jest uruchomiona (w razie konieczności zainstaluj nmap).

```
root@dlp:~# nmap localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-01 19:38 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@dlp:~#
```

6. Dodaj użytkownika `adduser sshuser`

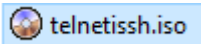
Ustaw hasło `passwd sshuser` na `1`

Część 2 - Konfiguracja Windows i klienta SSH dla Windows.

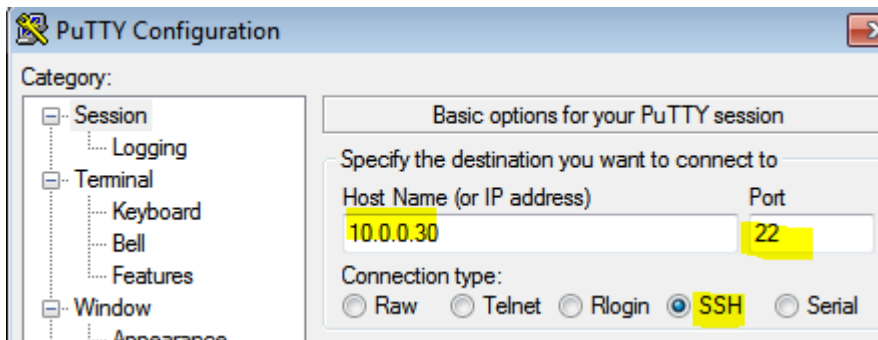
1. W Windows wykonaj dla karty sieciowej konfiguracje protokołu TCP/IPv4.

DHCP włączone	Nie
Adres IPv4	10.0.0.51
Maska podsieci IPv4	255.255.255.0
Brama domyślna IPv4	10.0.0.30
Serwer DNS IPv4	10.0.0.30

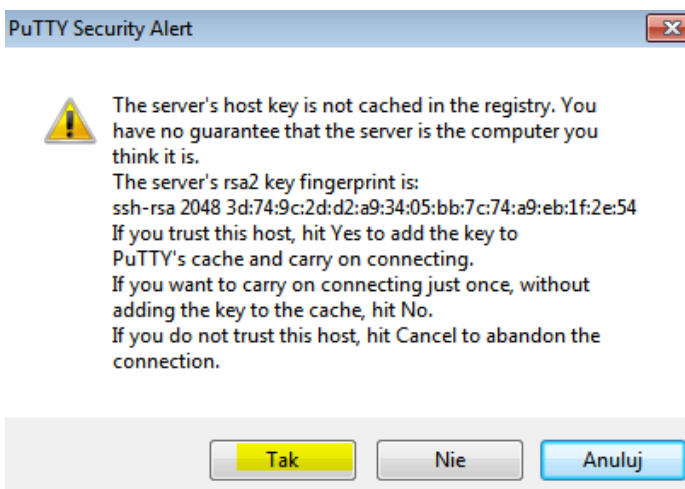
2. Podłącz wirtualny cd



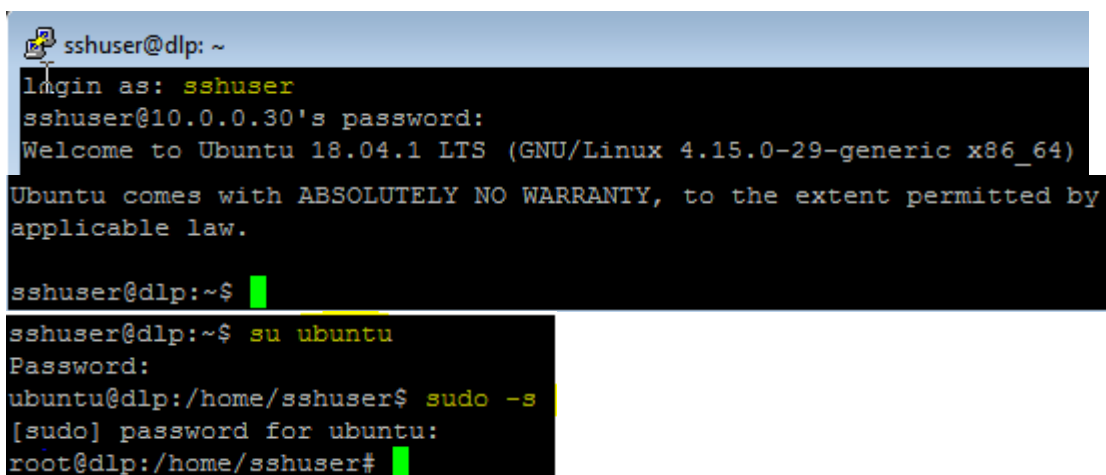
3. Korzystając z Putty skonfiguruj sesje ssh.



4. Otwórz sesje ssh.



5. Zaloguj się jako użytkownik **sshuser** z hasłem.



Zakończ sesje **exit**.

6. Podejmij próbę zalogowania się jako użytkownik **root** z hasłem 1234.

```
10.0.0.30 - PuTTY
login as: root
root@10.0.0.30's password:
Access denied
root@10.0.0.30's password: █
```

Podaj wnioski z wykonania powyższego ćwiczenia.

Część 3 - Konfiguracja i testowanie serwera SSH dla Ubuntu serwer.

1. Sprawdź na serwerze opcję umożliwiającą zalogowanie jako root.

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

```
GNU nano 2.9.3 /etc/ssh/sshd_config
#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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Uwierzytelnianie haseł dla OpenSSH Server na Ubuntu jest domyślnie włączone, więc możliwe jest logowanie bez zmiany jakichkolwiek ustawień. Ponadto konto root jest domyślnie zabronione. Uwierzytelnianie za pomocą hasła "PermitRootLogin prohibit-password", więc ustawienie domyślne jest dobre do użycia.

2. Aby zabronić logowania do root'a, zmień w następujący sposób w pliku /etc/ssh/ssdd_config opcję umożliwiającą zalogowanie jako root jak poniżej.

```
PermitRootLogin no
```

Wykonaj `systemctl restart ssh`

3. Przejdź na Windows. Otwórz sesję ssh, wykonaj próbę zalogowania się jako użytkownik **root** z hasłem. Korzystając z su przejdź do użytkownika root.

```
root@dlp: /home/sshuser
login as: sshuser
sshuser@10.0.0.30's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)
sshuser@dlp:~$ su ubuntu
Password:
ubuntu@dlp:/home/sshuser$ sudo -s
[sudo] password for ubuntu:
root@dlp:/home/sshuser#
```

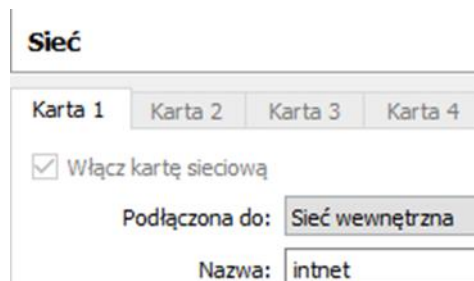
Podaj wnioski z wykonania powyższego ćwiczenia.

Część 4 – Instalacja i konfigurowanie, testowanie klienta SSH dla Ubuntu desktop.

Przygotuj maszynę z Ubuntu desktop.

1. Zainstaluj klienta SSH dla Ubuntu desktop.

```
ubuntu desktop (Migawka 1) [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
root@bolek-VirtualBox:~# apt -y install openssh-client
```



Ubuntu desktop Karta 1 zmień na

2. Zmień adres IP dla Ubuntu na **enp0s3** na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe **nano /etc/netplan/0** wciskasz tabulator. Pozostaw zalecane wpisy w tym pliku

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.0.53/24]
```

Zastosuj ustawienia

netplan apply

```
root@bolek-VirtualBox:~# netplan apply
```

Wyświetl ustawienia karty za pomocą `ip a`

```
root@bolek-VirtualBox:~# ip a |grep 10.0.0.53
    inet 10.0.0.53/24 brd 10.0.0.255 scope global enp0s3
```

3. Połącz się z serwerem SSH za pomocą zwykłego użytkownika.

```
root@bolek-VirtualBox:~# ssh ubuntu@10.0.0.30
The authenticity of host '10.0.0.30 (10.0.0.30)' can't be established.
ECDSA key fingerprint is SHA256:I2/syI68V386KQTcsZ1HpUqMfwNFM8+m6K60jafW13E
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
ubuntu@10.0.0.30's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)

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

System information as of Sun Sep 30 23:56:56 CEST 2018

System load:  0.0               Processes:           99
Usage of /:   0.2% of 914.76GB   Users logged in:    2
Memory usage: 16%              IP address for enp0s3: 10.0.2.15
Swap usage:   0%               IP address for enp0s8: 10.0.0.30

67 packages can be updated.
37 updates are security updates.

Last login: Sun Sep 30 22:07:42 2018
ubuntu@dlp:~$ _
```

4. Zakończ sesję i powtórnie połącz się z serwerem SSH za pomocą zwykłego użytkownika.

```

root@bolek-VirtualBox:~# ssh ubuntu@10.0.0.30
ubuntu@10.0.0.30's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)

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

System information as of Mon Oct  1 00:01:28 CEST 2018

System load:  0.04          Processes:           101
Usage of /:   0.2% of 914.76GB Users logged in:    2
Memory usage: 16%          IP address for enp0s3: 10.0.2.15
Swap usage:   0%           IP address for enp0s8: 10.0.0.30

67 packages can be updated.
37 updates are security updates.

Last login: Sun Sep 30 23:56:57 2018 from 10.0.0.53
ubuntu@dlp:~$ _

```

5. Sprawdź poleceniem NETSTAT aktywne połączenia protokołu TCP, czy jest otwarty port 22 odpowiadający za ssh z 10.0.0.53.

```

root@dlp:~# netstat -ant | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp        0      0 10.0.0.30:22       10.0.0.53:53110     ESTABLISHED
tcp        0      0 10.0.0.30:22       10.0.0.51:49167     ESTABLISHED
tcp6       0      0 :::22             :::*                 LISTEN

```

6. Wyświetl poleceniem komendy ssh na zdalnym hoście plik /etc/passwd.

```

root@bolek-VirtualBox:~# ssh ubuntu@10.0.0.30 "cat /etc/passwd"
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
telnetd:x:110:116:/:nonexistent:/usr/sbin/nologin
teluser:x:1001:1001:,,,:/home/teluser:/bin/bash
sshd:x:111:65534:/:run/sshd:/usr/sbin/nologin
sshuser:x:1002:1002:,,,:/home/sshuser:/bin/bash

```

Podaj wnioski z wykonania powyższego ćwiczenia.

Zakończ sesję.

Część 5 - Przesyłanie plików za pomocą klienta SSH dla Ubuntu desktop.

Przykład korzystanie z SCP (Secure Copy).

1. Utwórz plik tekst.txt


```
bolek@bolek-VirtualBox:~$ touch test.txt
```

2. Przekopiuj plik tekst.txt z lokalnego Ubuntu na zdalny serwer.

```
bolek@bolek-VirtualBox:~$ scp ./test.txt sshuser@10.0.0.30:~/
The authenticity of host '10.0.0.30 (10.0.0.30)' can't be established.
ECDSA key fingerprint is SHA256:I2/syI68V386KQTcsZ1HpUqMfwNFM8+m6K60jafW13E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
sshuser@10.0.0.30's password:
Permission denied, please try again.
sshuser@10.0.0.30's password:
test.txt                                100% 0    0.0KB/s  00:00
bolek@bolek-VirtualBox:~$ _
```

3. Przekopiuj plik tekst.txt z zdalnego serwera na lokalne Ubuntu.

```
bolek@bolek-VirtualBox:~$ scp sshuser@10.0.0.30:~/test.txt ./test.txt
sshuser@10.0.0.30's password:
test.txt                                100% 0    0.0KB/s  00:00
```

Przykład użycia SFTP (SSH File Transfer Protocol).

Funkcja serwera SFTP jest w [/etc/ssh/sshd_config] linia [Subsystem sftp /usr/lib/openssh/sftp-server].

4. Połącz się z zasobem sftp na zdalnym serwerze (`sftp sshuser@10.0.0.30`).
5. Pokaż aktualny katalog na zdalnym serwerze (`pwd`).
6. Pokaż aktualny katalog na serwerze lokalnie (`!pwd`).
7. Pokaż pliki w bieżącym katalogu na serwerze FTP (`ls -l`).
8. Pokaż pliki w bieżącym katalogu na serwerze lokalnie (`!!s -l`).

```
bolek@bolek-VirtualBox:~$ sftp sshuser@10.0.0.30
sshuser@10.0.0.30's password:
Connected to 10.0.0.30.
sftp> pwd
Remote working directory: /home/sshuser
sftp> !pwd
/home/bolek
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser    0 Oct  1 00:09 test.txt
sftp> !!s -l
razem 48
drwxr-xr-x  2 bolek bolek 4096 sie 28 14:58 Dokumenty
```

9. Utwórz katalog `public_html`
10. Przejdź do katalogu `public_html`
11. Pokaż aktualny katalog na zdalnym serwerze (`pwd`).

```
sftp> mkdir public_html
sftp> cd public_html
sftp> pwd
Remote working directory: /home/sshuser/public_html
```

12. Prześlij plik test.txt z zmianą jego nazwy do zdalnego serwera.

```
sftp> put test.txt ubuntuuser.txt
Uploading test.txt to /home/sshuser/public_html/ubuntuuser.txt
test.txt                                     100% 0    0.0KB/s   00:00
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:19 ubuntuuser.txt
```

13. Prześlij jakiś plik txt do zdalnego serwera.

```
sftp> put *.txt
Uploading test.txt to /home/sshuser/public_html/test.txt
test.txt                                     100% 0    0.0KB/s   00:00
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:20 test.txt
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:19 ubuntuuser.txt
```

14. Pobierz plik test.txt z zdalnego serwera.

```
sftp> get test.txt
Fetching /home/sshuser/public_html/test.txt to test.txt
```

15. Pobierz jakiś plik txt z zdalnego serwera.

```
sftp> get *.txt
Fetching /home/sshuser/public_html/test.txt to test.txt
Fetching /home/sshuser/public_html/ubuntuuser.txt to ubuntuuser.txt
```

16. Utwórz katalog testdir na zdalnym serwerze.

```
sftp> mkdir testdir
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:20 test.txt
drwxrwxr-x  2 sshuser  sshuser        4096 Oct  1 00:23 testdir
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:19 ubuntuuser.txt
```

17. Usuń katalog testdir na zdalnym serwerze.

```
sftp> rmdir testdir
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:20 test.txt
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:19 ubuntuuser.txt
```

18. Usuń plik debian.txt na zdalnym serwerze.

```
sftp> rm ubuntuuser.txt
Removing /home/sshuser/public_html/ubuntuuser.txt
sftp> ls -l
-rw-rw-r--  1 sshuser  sshuser          0 Oct  1 00:20 test.txt
```

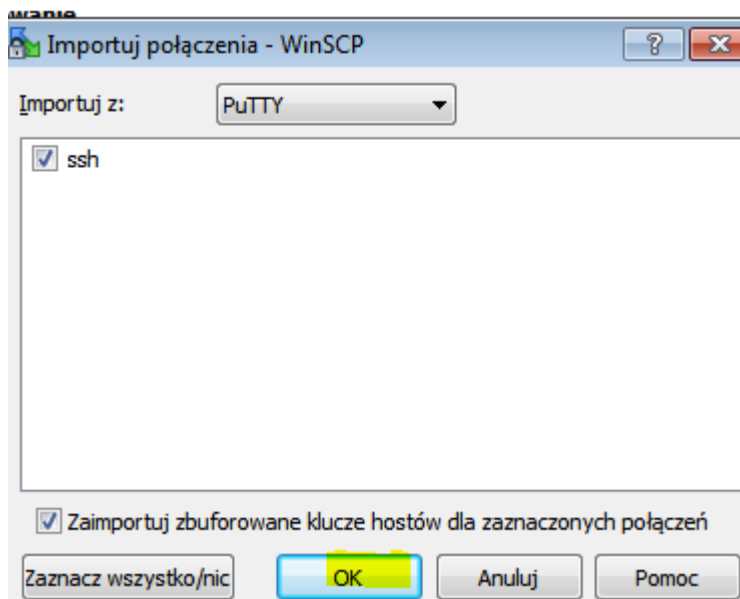
19. Zakończ połączenie z zdalnym serwerem.

```
sftp> quit
bolek@bolek-VirtualBox:~$
```

Podaj wnioski z wykonania powyższego ćwiczenia.

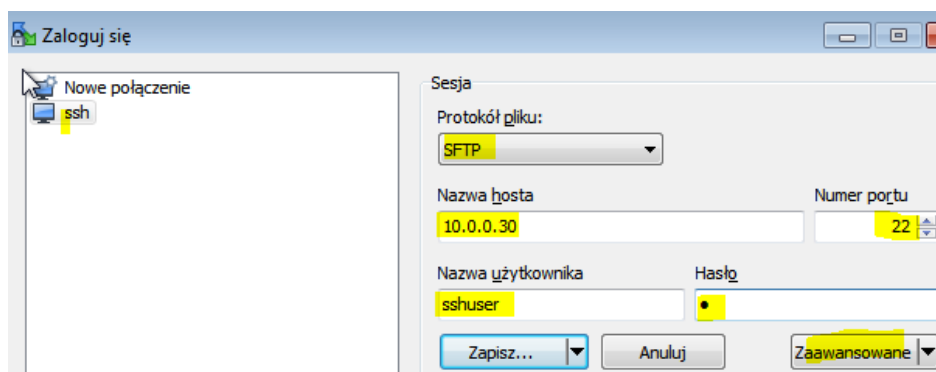
Część 6 – Konfiguracja przesyłanie plików za pomocą klienta SSH dla Windows.

1. Pobierz, zainstaluj i uruchom WinSCP, importuj połączenia

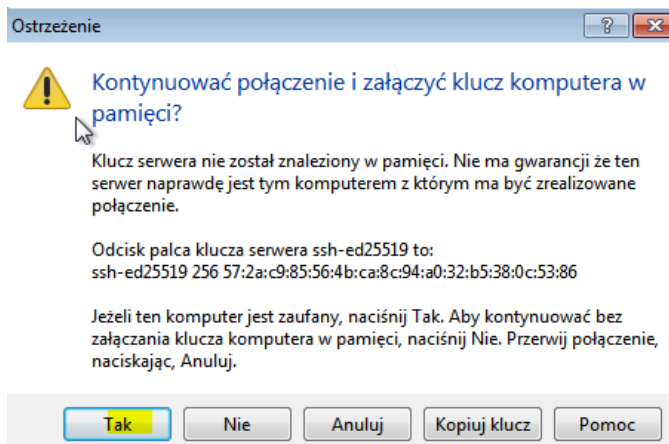
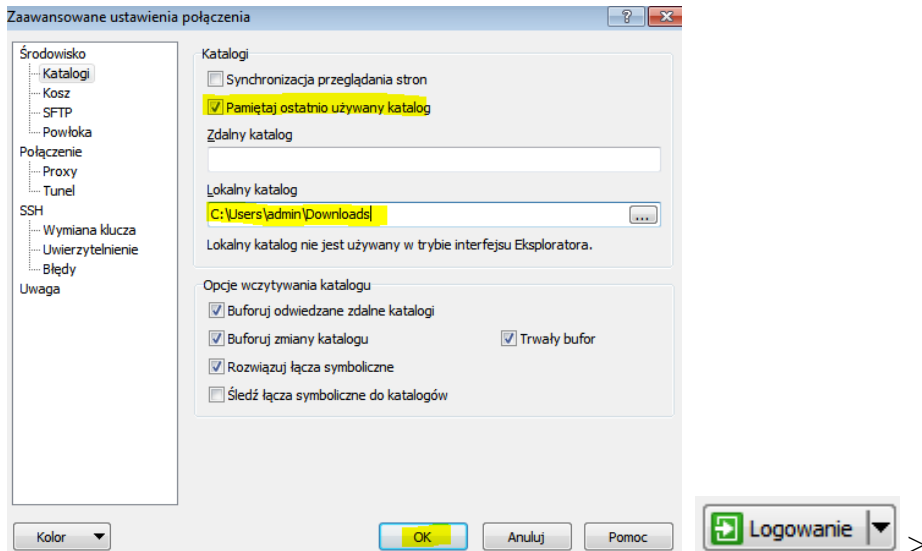


2. Jeżeli nie będzie ekranu jak poniżej kliknij przycisk "Nowy".

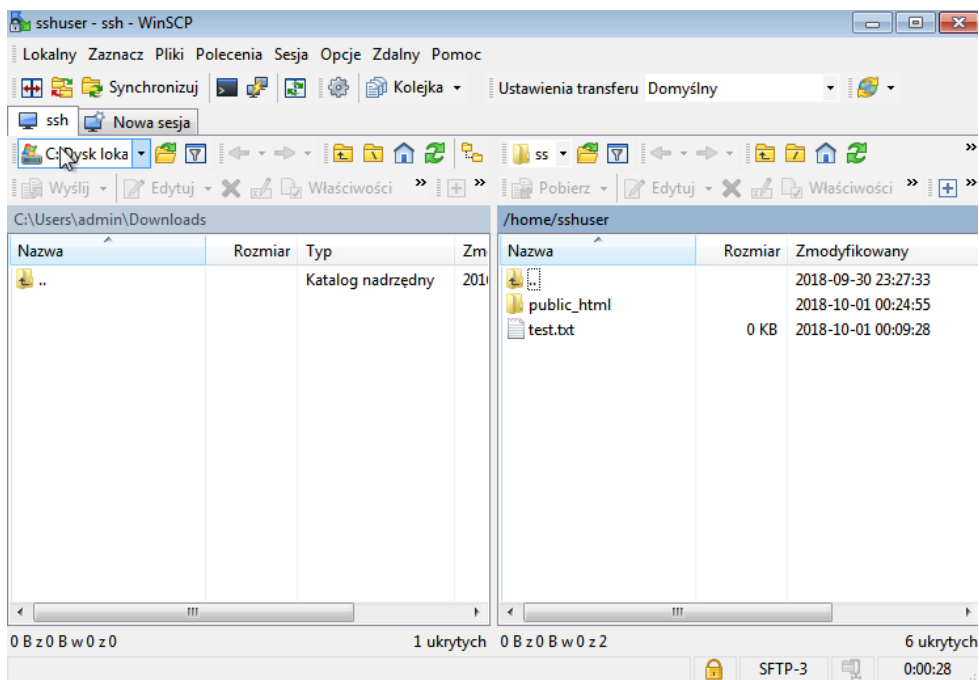
3. Na ekranie wyświetlane są informacje służące, aby się zalogować, uzupełnij je (wprowadź hasło logowania użytkownika), wybierz Zaawansowane.



4. Przejdź do sekcji "Katalogi" w menu po lewej stronie. Pozostaw zdalny katalog serwera i lokalny katalog klienta jak poniżej. W celu zalogowania kliknij przycisk logowania w następnym oknie.



5. Po zalogowaniu możliwe jest przesyłanie i pobieranie plików.



Podaj wnioski z wykonania powyższego ćwiczenia.

Część 7 - Uwierzytelnianie SSH Key-Pair dla klienta systemu Linux.

Konfiguracja serwera SSH do logowania z uwierzytelnianiem Key-Pair.

1. Utwórz klucz prywatny do klienta oraz klucz publiczny do serwera. Parę kluczy tworzymy dla każdego użytkownika.

a) Zaloguj się za pomocą zwykłego użytkownika i postępuj, jak następuje.

```
root@d1p:~# su ubuntu
ubuntu@d1p:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_rsa):
Created directory '/home/ubuntu/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_rsa.
Your public key has been saved in /home/ubuntu/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:DS30i6xhY1N6tZJ9m8d2hL3hAE9EVZjsgrIkadWsn0k ubuntu@d1p
The key's randomart image is:
+---[RSA 2048]---+
|      .o  .o.+o|
|     ..oo  .+ |
|    +++o... |
|   ++B=.o... |
|  .B+So+ +. o |
| o *Eo . o..o|
| . o o ..o.o|
| . . . o+o.|
|      oo . |
+----[SHA256]-----+
```

b) Zmień nazwę pliku i prawa do pliku.

```
ubuntu@d1p:~$ mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
ubuntu@d1p:~$ chmod 600 ~/.ssh/authorized_keys
```

Przenieś tajny klucz utworzony na serwerze do klienta, aby zalogować się za pomocą uwierzytelniania kluczy.

Na kliencie (Linux) **Ubuntu desktop**.

2. Utwórz konto zwykłego użytkownika i zaloguj się do niego.

3. Utwórz lokalnie katalog domowy dla ssh.

4. Ustaw wszystkie prawa tylko dla katalogu domowego użytkownika, dla grupy i innych brak praw.

```
root@bolek-VirtualBox:/home# adduser ucze
root@bolek-VirtualBox:/home# su ucze
ucze@bolek-VirtualBox:/home$ mkdir ~/.ssh
ucze@bolek-VirtualBox:/home$ chmod 700 ~/.ssh
```

5. Skopiuj tajny klucz do lokalnego katalogu ssh (hasło 1234).

```
ucze@bolek-VirtualBox:/home$ scp ubuntu@10.0.0.30:/home/ubuntu/.ssh/id_rsa ~/.ssh
The authenticity of host '10.0.0.30 (10.0.0.30)' can't be established.
ECDSA key fingerprint is SHA256:I2/syI68V386KQTcsZ1HpUqMfwNFM8+m6K60jafW13E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
sshuser@10.0.0.30's password: ●
id_rsa 100% 1679 252.6KB/s 00:00
```

6. Połącz się z klienta lokalnego przez ssh do zdalnego serwera 10.0.0.30.

```
ucze@bolek-VirtualBox:/home$ ssh ubuntu@10.0.0.30
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)

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

System information as of Mon Oct  1 00:58:16 CEST 2018

System load:  0.01          Processes:            98
Usage of /:   0.2% of 914.76GB Users logged in:     1
Memory usage: 16%          IP address for enp0s3: 10.0.2.15
Swap usage:   0%           IP address for enp0s8: 10.0.0.30

67 packages can be updated.
37 updates are security updates.

Last login: Mon Oct  1 00:01:29 2018 from 10.0.0.53
ubuntu@d1p:~$ _
```

7. W wierszu 56 ustaw "PasswordAuthentication no", to jest bardziej bezpieczne.

```
root@debian:~# nano /etc/ssh/sshd_config
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

systemctl restart ssh

Podaj wnioski z wykonania powyższego ćwiczenia.

Część 8 - Uwierzytelnianie SSH Key-Pair dla klienta systemu Windows.

Skonfiguruj serwer SSH, aby zalogować się za pomocą klucza prywatnego i klucza publicznego klienta dla serwera. Tworzenie pary kluczy dla użytkownika wykonałeś wcześniej.

1. Sprawdź ustawienia serwera ssh.

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PermitEmptyPasswords no
```

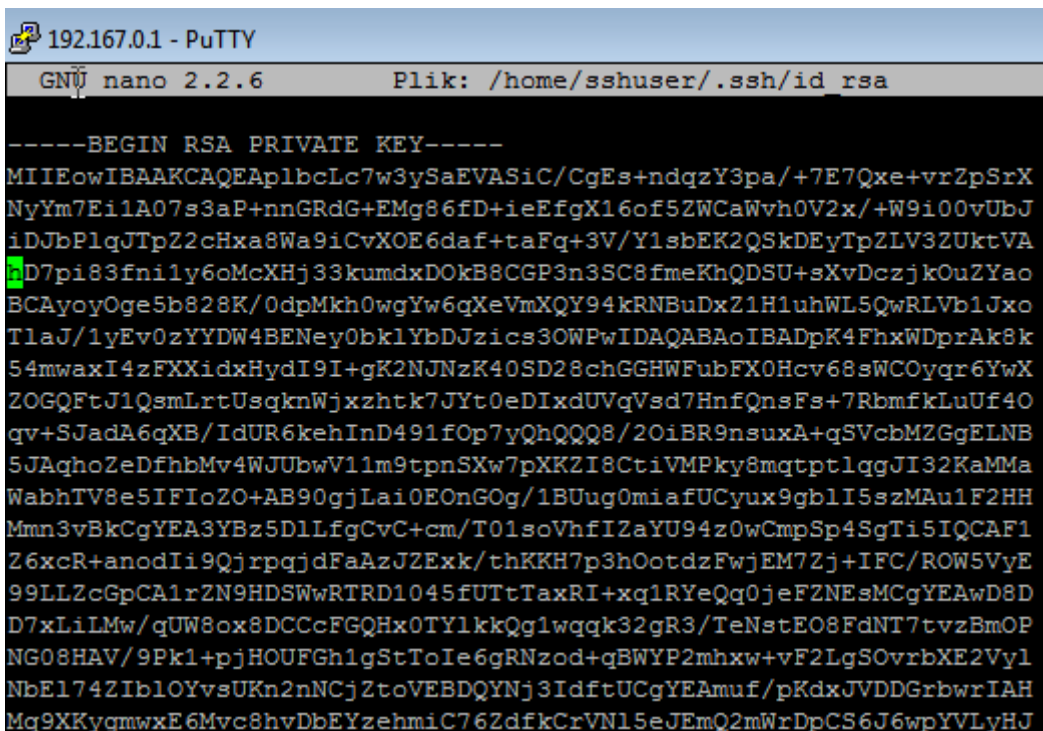
```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

Jeżeli jest potrzeba na serwerze wykonaj restart usługi. `/etc/init.d/ssh restart`

Zaloguj się do serwera SSH z klienta Windows.

a) edytuj plik `id_rsa`,

`nano /home/ubuntu/.ssh/id_rsa`



```
192.167.0.1 - PuTTY
GNU nano 2.2.6 Plik: /home/sshuser/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApIbcLc7w3ySaEVA5iC/CgEs+ndqzY3pa/+7E7Qxe+vrZpSrX
NyYm7Ei1A07s3aP+nnGRdG+EMg86fD+ieEfgX16of5ZWCaWvh0V2x/+W9i00vUbJ
iDjBPlqJTpZ2cHxa8Wa9iCvXOE6daf+taFq+3V/Y1sbEK2QSkDEyTpZLV3ZUktVA
D7pi83fn1y6oMcXHj33kumdxDOkB8CGP3n3SC8fmeKhQDSU+sXvDczjkOuZYao
BCAyoyOge5b828K/0dpMkh0wgYw6qXeVmXQY94kRNBUdxZ1H1uhWL5QwRLVb1Jxo
TlaJ/1yEv0zYYDW4BENey0bklYbDjzics3OWPwIDAQABAoIBADpK4FhxWDprAk8k
54mwaxI4zFXXidxHydI9I+gK2NjNzK40SD28chGGHWfubFX0Hcv68sWCOyqr6YwX
ZOGQFtJ1QsmLrtUsqknWjxzhtk7JYt0eDIxdUVqVsd7HnfQnsFs+7RbmfkLuUf40
qv+SJadA6qXB/IdUR6kehInD491fOp7yQhQQQ8/2OiBR9nsuxA+qSVcbMZGgELNB
5JAqhoZeDfhhMv4WJUbwV11m9tpnSXw7pXKZI8CtiVMPky8mgtptlqgJI32KaMMA
WabhTV8e5IFIoZO+AB90gjLai0EOnGOg/1BUug0miafUCyux9gblI5szMAu1F2HH
Mmn3vBkCgYEA3YBz5DlLfgCvC+cm/T01soVhfIZaYU94z0wCmpSp4SgTi5IQCAF1
Z6xcR+anodIi9QjrpqjdFaAzJZExk/thKKH7p3hOotdzFwjEM7Zj+IFC/ROW5VyE
99LLZcGpCA1rZN9HDSWwRTRD1045fUTtTaxRI+Xq1RYeQq0jeFZNEsMCgYEAwD8D
D7xLiLMw/qUW8ox8DCCcFGQHx0TY1kkQg1wqqk32gR3/TeNstE08FdNT7tvzBmOP
NG08HAV/9Pk1+pjHOuFGH1gStToIe6gRNzod+qBWYP2mhxw+vF2LgSOvrbXE2Vy1
NbE174Zi1b0YvsUKn2nNCjZtoVEBDQYNj3IdftUCgYEAuf/pKdxJVDDGrbwrIAH
Mq9XKygmwxE6Mvc8hvDbEYzehmiC76ZdfkCrVN15eJEmQ2mWrDpCS6J6wpYVLYHJ
```

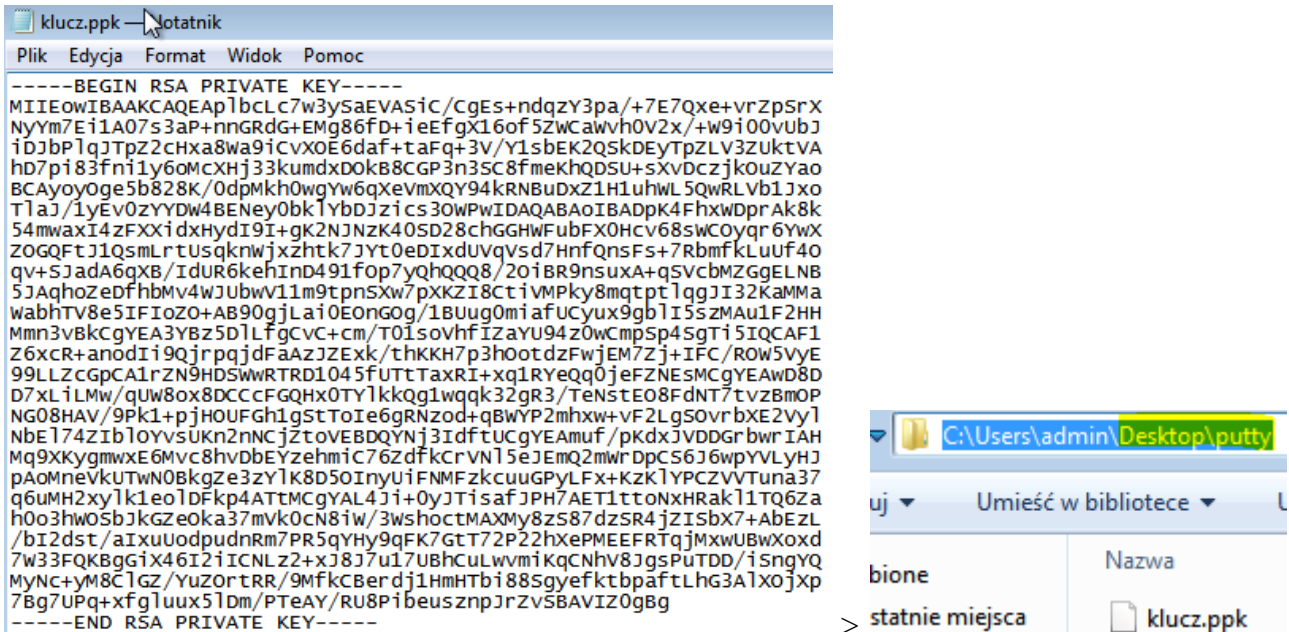


```

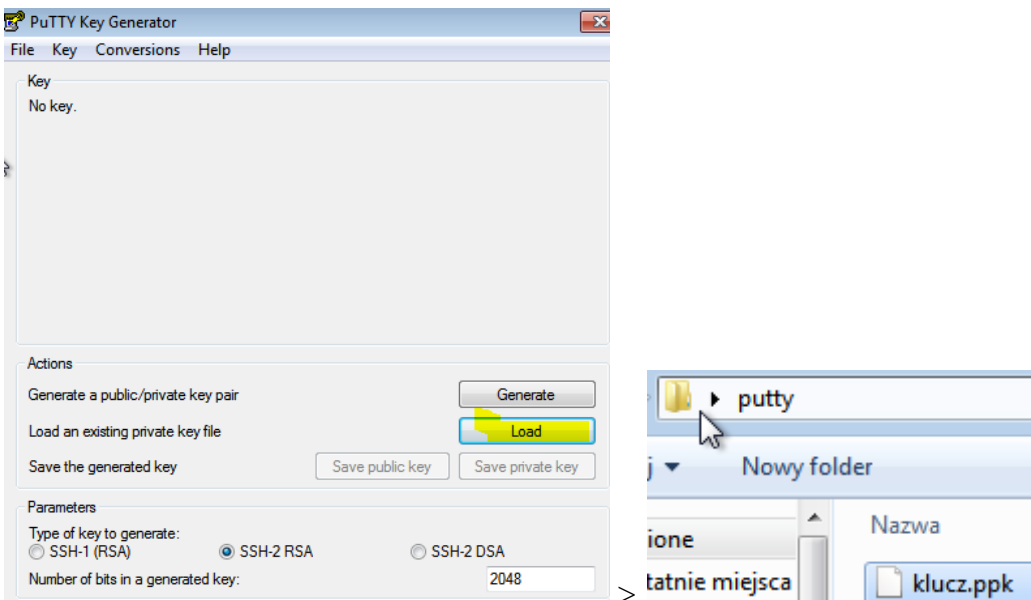
pAoMneVkuTWn0BkgZe3zYlK8D50InyUiFNMfZkcUuGPyLFx+KzKlYPCZVVTuna37
q6uMH2xylkleolDFkp4ATtMCGYAL4Ji+0yJTisafJPH7AET1ttoNxHRakl1TQ6Za
h0o3hWOSbJkGZeOka37mVkc0cN8iW/3WshoctMAXMy8zS87dzSR4jZISbX7+AbEzL
/bI2dst/aIXuUodpudnRm7PR5qYHY9qFK7GtT72P22hXePMEEFRTqjMxwUBwXoxd
7W33FQKBGgix46I2iICNLz2+xJ8J7u17UBhCuLwvmiKqCNhV8JgsPuTDD/iSngYQ
MyNc+yM8ClGZ/YuZOrtRR/9MfkCBerdj1HmHTbi88SgyefktbpafLhG3AlX0jXp
7Bg7UPq+xfgluux5lDm/PTeAY/RU8PibeusznpJrZvSBAVIZ0gBg
-----END RSA PRIVATE KEY-----

```

b) Przekopij zawartość `id_rsa` do nowo utworzonego w Windows (`Desktop\putty`) pliku `klucz.ppk`.

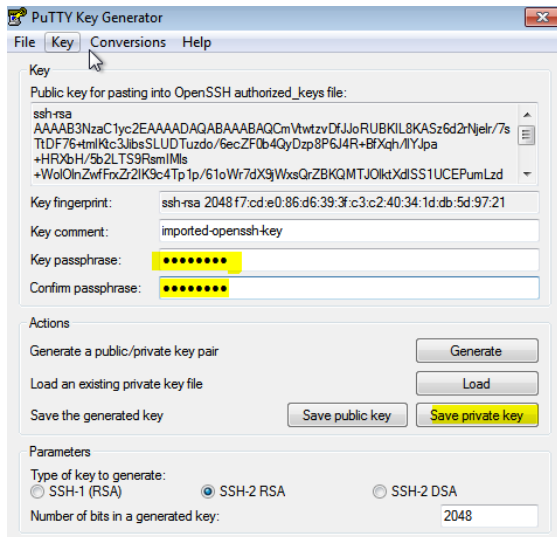


c) Uruchom "Puttygen.exe" z materiałów i kliknij przycisk "Load".



d) Zmodyfikuj tajny klucz, który został pobrany, hasło jest wymagane. Podaj hasło np `4321`.

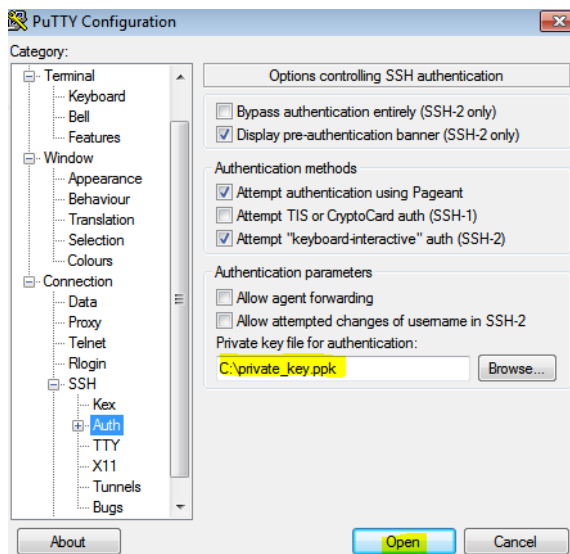
e) Kliknij "Save private key", aby zapisać je w folderze z dowolną nazwą pliku np. `C:\private_key.ppk`.



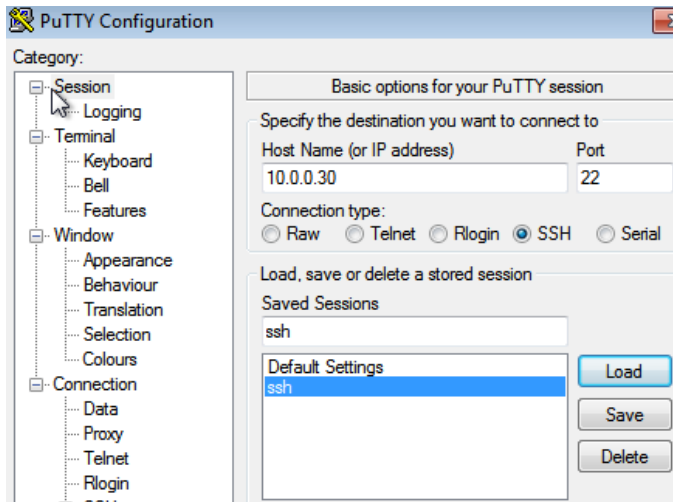
Nie generuj klucza. Nie zmieniaj wartości "Number of bits In a generated key".

Podczas generowania certyfikatów ustawienie jak na zrzucie poniżej powoduje długi czas tworzenia certyfikatów.

2. Uruchom Putty i otwórz [Połączenie] - [SSH] - [Auth] w menu po lewej stronie, a następnie wybierz "private_key", który został właśnie zapisany powyżej.



3. Powróć do [Session] w lewym menu i połącz się z serwerem SSH.



4. Hasło jest wymagane, podaj hasło **zaq1@WSX** a następnie jest ono odebrane i sprawdzane. Jeśli hasło jest poprawne, to zalogowanie jest możliwe. **ubuntu**

```
ubuntu@d1p: ~
login as: ubuntu
Authenticating with public key "imported-openssh-key"
Passphrase For key "imported-openssh-key":
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-29-generic x86_64)

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

System information as of Mon Oct  1 22:45:00 CEST 2018

System load:  0.0          Processes:    104
Usage of /:   0.2% of 914.76GB  Users logged in:  1
Memory usage: 16%          IP address for enp0s3: 10.0.2.15
Swap usage:  0%           IP address for enp0s8: 10.0.0.30

67 packages can be updated.
37 updates are security updates.

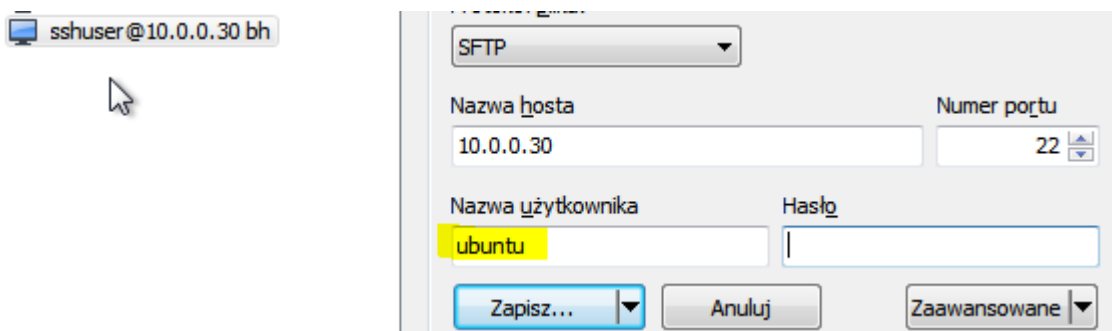
Last login: Mon Oct  1 22:38:22 2018 from 10.0.0.51
ubuntu@d1p:~$
```

5. Pokaż aktualny katalog na zdalnym serwerze (**pwd**).
6. Pokaż pliki w bieżącym katalogu na serwerze FTP (**ls -la**).

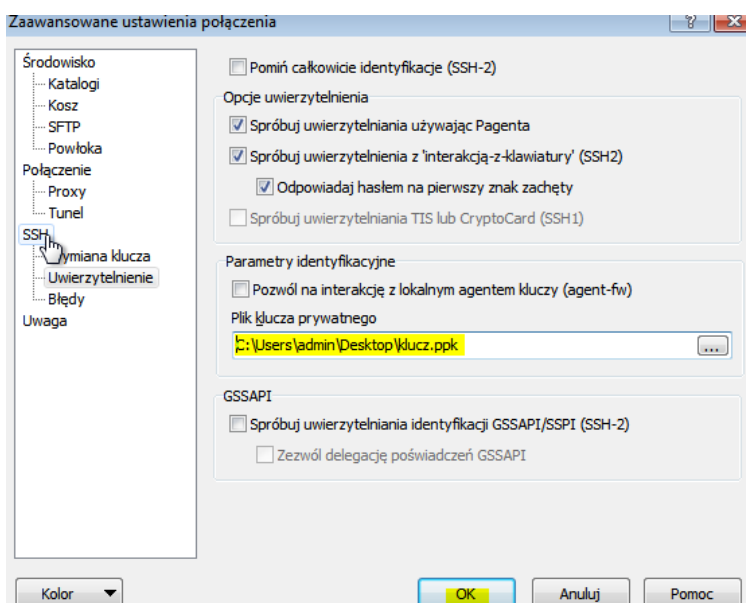
```
ubuntu@dlp:~$ pwd
/home/ubuntu
ubuntu@dlp:~$ ls -la
total 48
drwxr-xr-x 6 ubuntu ubuntu 4096 Oct  1 22:39 .
drwxr-xr-x 4 root    root    4096 Oct  1 20:27 ..
-rw-r----- 1 root    root     271 Oct  1 21:00 .bash_history
-rw-r--r--  1 ubuntu ubuntu   220 Aug 28 14:33 .bash_logout
-rw-r--r--  1 ubuntu ubuntu  3771 Aug 28 14:33 .bashrc
drwx----- 2 ubuntu ubuntu  4096 Aug 28 14:35 .cache
drwx----- 3 ubuntu ubuntu  4096 Aug 28 14:35 .gnupg
drwxrwxr-x  3 ubuntu ubuntu  4096 Oct  1 22:39 .local
-rw-r--r--  1 root    root      10 Oct  1 21:38 .nanorc
-rw-r--r--  1 ubuntu ubuntu   807 Aug 28 14:33 .profile
drwx----- 2 ubuntu ubuntu  4096 Oct  1 22:41 .ssh
-rw-r--r--  1 ubuntu ubuntu     0 Aug 28 14:36 .sudo_as_admin_successful
-rw-r----- 1 root    root     997 Oct  1 21:43 .viminfo
```

7. Korzystając z WinScp zaloguj się do hosta - serwera 10.0.0.30.

a) Ustaw parametry sesji i użytkownika.



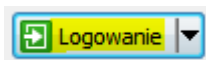
b) Podłącz plik klucza prywatnego.



c) Zapisz sesję jak poniżej.

> ssh10.0.0.30

d) Zaloguj się (połącz się z serwerem SSH 10.0.0.30).

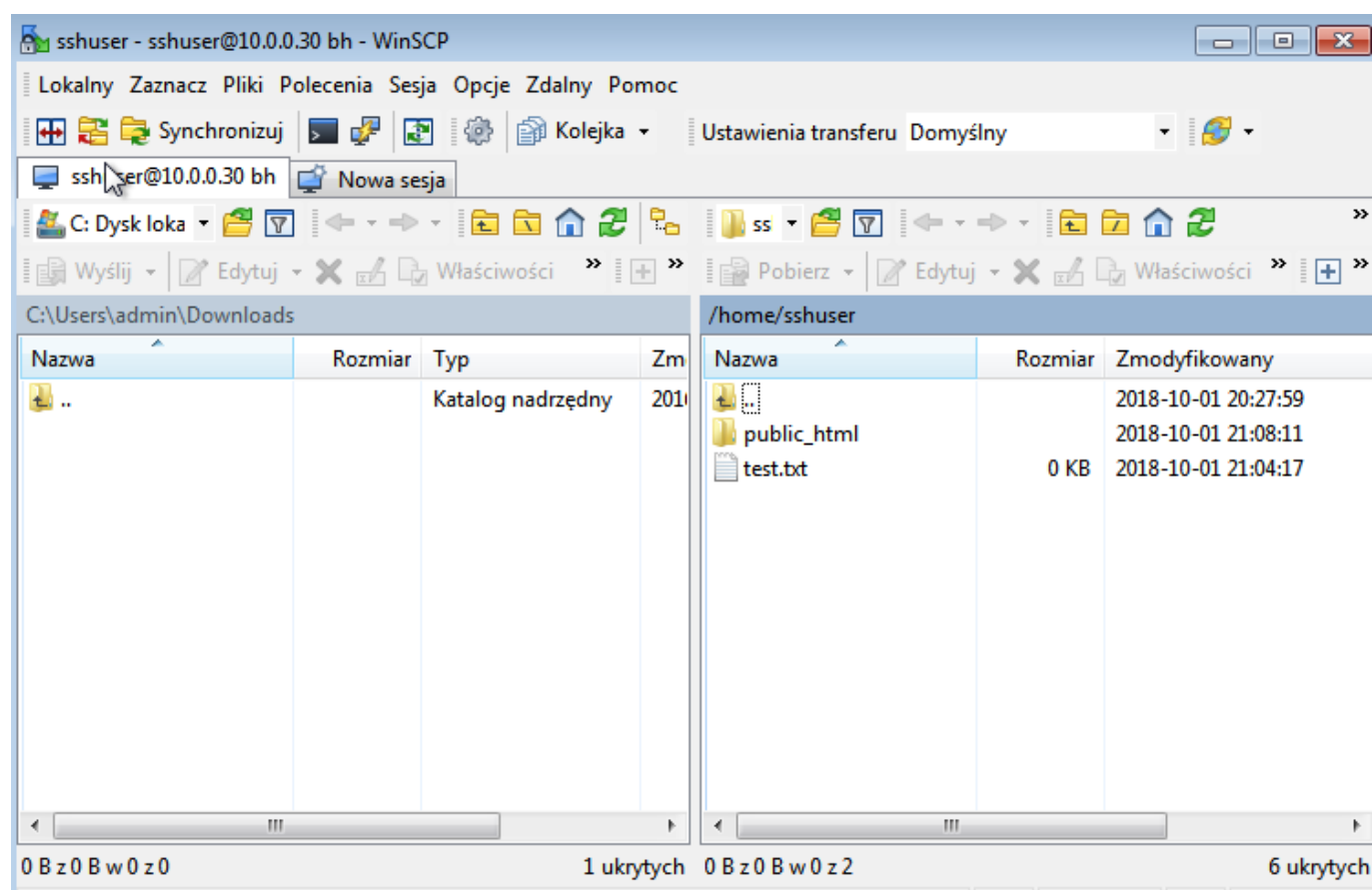


8. Wprowadź hasło dla klucza.

a) Hasło jest wymagane, podaj hasło **4321** następnie jest ono odebrane i sprawdzane.

Jeśli hasło jest poprawne, to zalogowanie jest możliwe.

b) Efekt końcowy.



Podaj wnioski z wykonania powyższego ćwiczenia.

Jeśli twój Windows to Windows 10 w wersji 1803, klient OpenSSH został zaimplementowany jako funkcja Windows, więc możliwe jest uwierzytelnienie za pomocą pary kluczy SSH bez Putty i innych programów. Przenieś tajny klucz do systemu Windows 10 i umieść go w folderze [(zaloguj się do folderu domowego użytkownika) \. Ssh] a ssh będzie gotowy do użycia logowania z parą kluczy.