Instalacja i konfiguracja serwera SSH.

Cel ogólny lekcji: Nauczanie instalacji i konfiguracji serwera SSH dla Ubuntu serwer oraz klienta SSH dla Windows oraz Linux i zdobycie umiejętności korzystania z SSH.

Cele szczegółowe:

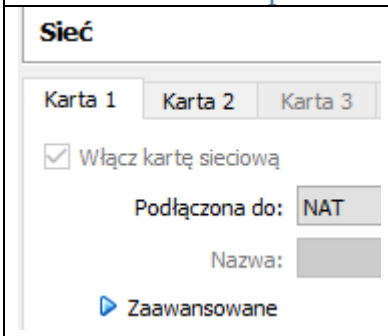
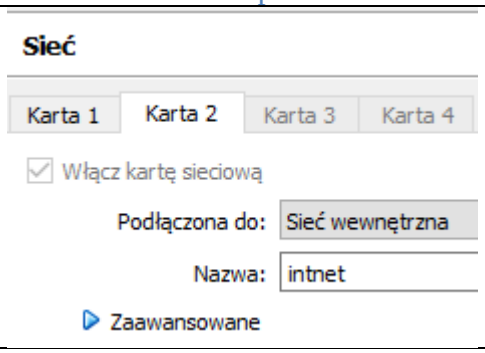
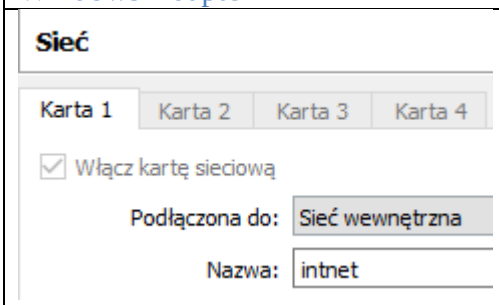
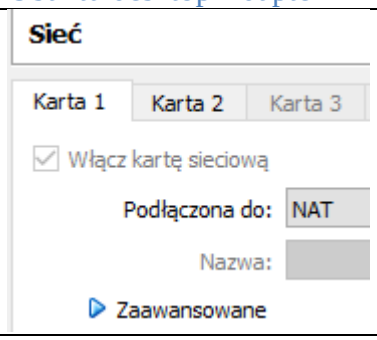
1. Wyjaśnienie pojęć związanych z SSH.
2. Instalacja serwera SSH na Ubuntu serwer.
3. Uruchomienie i zatrzymanie usług sieciowych na Ubuntu serwer.
4. Konfiguracja serwera SSH na Ubuntu serwer.
5. Korzystanie z SSH na Ubuntu serwer.
6. Udzielanie odpowiedzi na pytania związane z zadaniami.
7. Ustalenie statycznego adresu IP dla interfejsu sieciowego enp0s8 (Adapter 2) na Ubuntu serwer.
8. Wyświetlenie domyślnej bramy dla interfejsów sieciowych na Ubuntu serwer.
9. Zatrzymanie i uruchomienie usługi SSH na Ubuntu serwer.
10. Restart usługi SSH na Ubuntu serwer.
11. Sprawdzenie czy port 22 odpowiadający za SSH jest otwarty przez polecenie NETSTAT na Ubuntu serwer.
12. Sprawdzenie czy usługa SSH jest uruchomiona na Ubuntu serwer.
13. Dodanie użytkownika na Ubuntu serwer.
14. Ustawienie hasła dla użytkownika na Ubuntu serwer.
15. Konfiguracja protokołu TCP/IPv4 dla karty sieciowej w Windows.
16. Otwarcie sesji SSH na Windows.
17. Zalogowanie się jako użytkownik SSH na Windows.
18. Zmiana użytkownika bieżącego na Ubuntu, a następnie na root-a w Windows.
19. Zakończenie sesji SSH w Windows.

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.

Przywróć migawkę „Migawka 1” zawierającą przygotowane do ćwiczeń maszyny Ubuntu serwer i desktop (klient) oraz Windows desktop (klient)

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 serwer i klienty zgodnie z wymaganiami w instrukcji.

Ubuntu serwer Adapter 1	Ubuntu serwer Adapter 2
	
Windows Adapter 1	**Ubuntu desktop Adapter 1**
	

Po uruchomieniu Ubuntu serwer
podaj **login**: root **Password**: 1234

```
ubuntusrv login: root
Password:
Welcome to Ubuntu 20.04 LTS
```
>
```
root@ubuntusrv:~#
```

lub
podaj **login**: ubuntu **Password**: ubuntu
Wisz sudo -s **Password**: ubuntu

```
ubuntu@ubuntusrv:~$ sudo -s
[sudo] password for ubuntu:
root@ubuntusrv:/home/ubuntu#
```

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

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

```
root@ubuntusrv:~# 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:febe:d52b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:be:d5:2b  txqueuelen 1000  (Ethernet)
        RX packets 195929  bytes 258698845 (258.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16647  bytes 1045394 (1.0 MB)
        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 – nazwa pliku zostanie uzupełniona do postaci *.yaml
Pozostaw zalecane wpisy w tym pliku jak poniżej, pamiętaj o dokładności wpisów

```
# This is the network config wri
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      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 rutera) 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 aktualizację apt update - aktualizowanie listy pakietów i repozytoriów

Jeśli pojawi się `Run 'apt list --upgradable' to see them.` można instalować poniższy pakiet.

2. Wykonaj `root@ubuntusrv:~# apt -y install openssh-server`

Jeśli nie jest możliwe należy zapytać prowadzącego czy można wykonać apt-get upgrade - aktualizacja systemu.

3. Kolejno zatrzymaj i uruchom usługę ssh

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

4. Zrestartuj usługę ssh

```
root@ubuntusrv:~# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
```

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

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

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

Jeśli nie jest zainstalowany to zainstaluj program nmap `root@ubuntusrv:~# apt -y install nmap`

```
root@ubuntusrv:~# nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-12 17:20 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

7. Dodaj użytkownika `adduser sshuser`

Ustaw hasło `passwd sshuser` na 1 (jeden)

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. Uruchom cmd

3. Otwórz sesje ssh,

4. Zaloguj się jako użytkownik sshuser z hasłem 1 (jeden).

```
C:\Users\admin>ssh sshuser@10.0.0.30
sshuser@10.0.0.30's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux
```

5. Zatwierdz klucz przez wpisanie yes i potwierdzenie przez enter
6. Za pomocą polecenia su zmień użytkownika bierzącego na ubuntu a następnie na root-a za pomocą polecenia sudo -s

```
sshuser@ubuntusrv:~$ su ubuntu
Password:
ubuntu@ubuntusrv:/home/sshuser$ sudo -s
[sudo] password for ubuntu:
root@ubuntusrv:/home/sshuser#
```

Zakończ sesje exit > exit > exit.

7. Podejmij próbę zalogowania się jako użytkownik root z hasłem 1234.

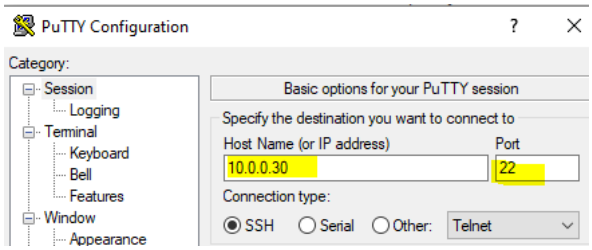
```
C:\Users\admin>ssh root@10.0.0.30
root@10.0.0.30's password:
Permission denied, please try again.
root@10.0.0.30's password:
```

8. Podaj wnioski z wykonania w cmd połączenia ssh w powyższym ćwiczeniu.

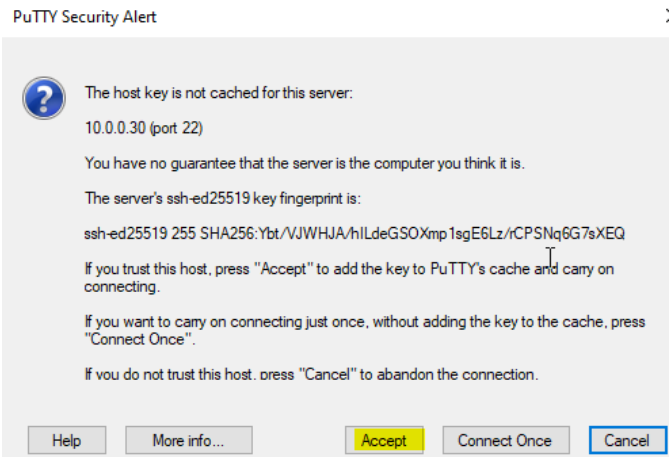
9. Pobierz z https://tiny.pl/wph9v i podłącz wirtualny cd

telnetissh.iso

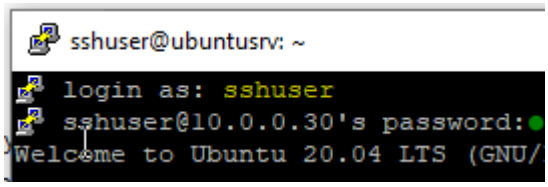
10. Korzystając z putty skonfiguruj sesje ssh.



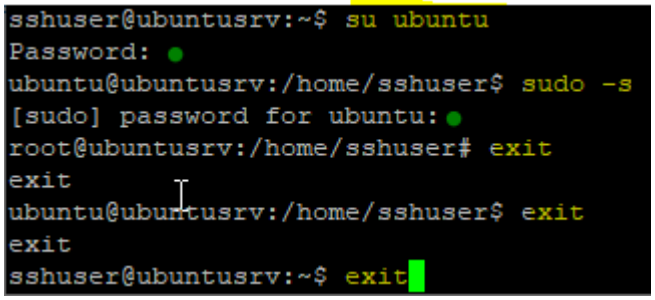
11. Zatwierdz klucz przez wybór Accept i potwierdzenie przez enter



12. Zaloguj się jako użytkownik sshuser z hasłem 1 (jeden).

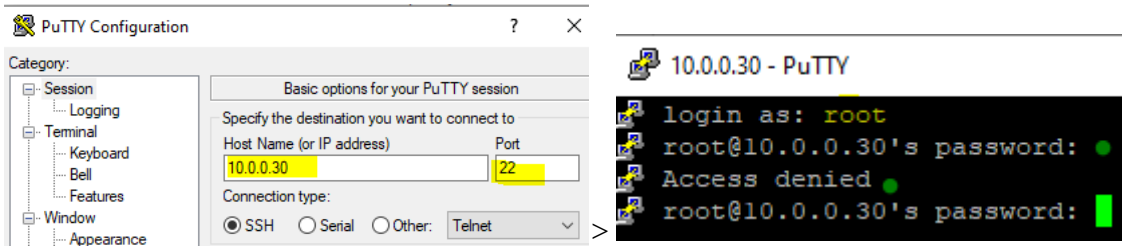


13. Za pomocą polecenia su zmień użytkownika bierzącego na ubuntu a następnie na root-a za pomocą polecenia sudo -s



Zakończ sesje.

14. Podejmij próbę zalogowania się jako użytkownik root z hasłem 1234.



15. Podaj wnioski z wykonania w putty połączenia ssh w powyższym ćwiczeniu.

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

1. Sprawdź na serwerze opcję umożliwiającą zalogowanie jako root.

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

```
# 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, w pliku /etc/ssh/ssdd_config zmień w następujący sposób opcję umożliwiającą zalogowanie jako root jak poniżej.

PermitRootLogin no

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
```

Wykonaj systemctl restart ssh

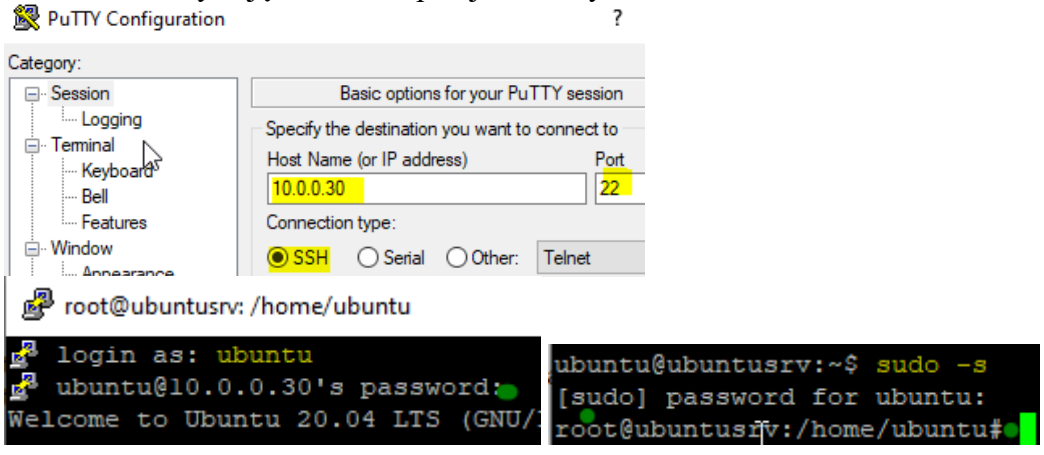
3. Przejdź na Windows. Otwórz w cmd sesje ssh, wykonaj próbę zalogowania się jako użytkownik root z hasłem. Korzystając z sudo -s przejdź do użytkownika root.

```
C:\Users\admin>ssh ubuntu@10.0.0.30
ubuntu@10.0.0.30's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linu
```

>

```
ubuntu@ubuntusrv:~$ sudo -s
[sudo] password for ubuntu:
root@ubuntusrv:/home/ubuntu#
```

4. Podaj wnioski z wykonania w cmd połączenia ssh w powyższym ćwiczeniu.
5. Przejdź na Windows. Otwórz w putty sesje ssh, wykonaj próbę zalogowania się jako użytkownik root z hasłem. Korzystając z sudo -s przejdź do użytkownika root.



6. Podaj wnioski z wykonania w putty połączenia ssh w powyższym ćwiczeniu.

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

Przygotuj maszynę z Ubuntu desktop.

1. Po uruchomieniu Ubuntu naciśnij Ctrl+Alt+F4 podaj **login**: ubuntu **Password**: ubuntu
Wisz sudo -s **Password**: ubuntu

```
ubuntu@ubunu2004:~$ sudo -s
root@ubunu2004:/home/ubuntu#
```

2. Sprawdź przydzielony automatycznie z NAT adres ip

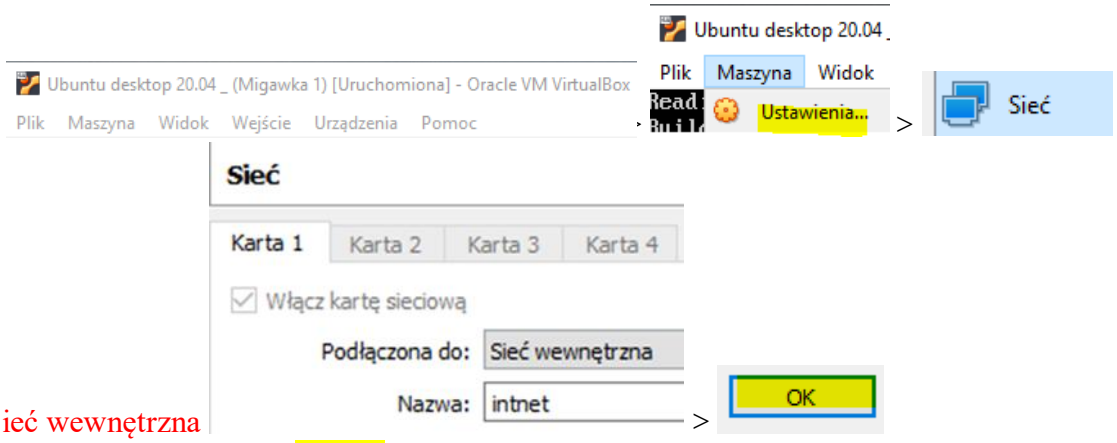
```
root@ubunu2004:/home/ubuntu# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 655
    link/loopback 00:00:00:00:00:00 b
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lf
    inet6 ::1/128 scope host
       valid_lft forever preferred_lf
2: enp0s3: <BROADCAST,MULTICAST,UP,LO
0
    link/ether 08:00:27:9a:ee:8e brd
    inet 10.0.2.15/24 brd 10.0.2.255
```

3. Wykonaj aktualizację apt update - aktualizowanie listy pakietów i repozytoriów

Jeśli pojawi się `Run 'apt list --upgradable' to see them.` można instalować poniższy pakiet.

4. Zainstaluj klienta SSH dla Ubuntu desktop.

```
root@ubunu2004:/home/ubuntu# apt -y install openssh-client
```

5. Ubuntu desktop 

Karta 1 zmień na Sieć wewnętrzna

6. Zmień adres IP dla Ubuntu desktop na enp0s3 na statyczny.

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

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
      addresses: [10.0.0.53/24]
```

b) Zastosuj ustawienia
netplan apply

```
root@ubunu2004:/home/ubuntu# netplan apply
```

c) Wyświetl ustawienia karty za pomocą ip a

```
root@ubunu2004:/home/ubuntu# ip a|grep 10.0.0.53
    inet 10.0.0.53/24 brd 10.0.0.255 scope global enp0s3
```

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

```
root@ubunu2004:/home/ubuntu# 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:tBAhyabVm526PiuKybuFfsoRou28q6QrRb8yAdVFf7U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)
```

```
Last login: Thu Jan 12
ubuntu@ubuntusrv:~$
```

8. Zakończ sesje (exit) i powtórnie połącz się z serwerem SSH za pomocą zwykłego użytkownika.

```
root@ubunu2004:/home/ubuntu# ssh ubuntu@10.0.0.30
ubuntu@10.0.0.30's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-ger
```

> `ubuntu@ubuntusrv:~$`

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

```
ubuntu@ubuntusrv:~$ 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            10.0.0.53:57758         ESTABLISHED
tcp        0      0 10.0.0.30:22            10.0.0.51:55743         ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
```

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

```
root@ubunu2004:/home/ubuntu# ssh ubuntu@10.0.0.30 "cat /etc/passwd"
ubuntu@10.0.0.30's password:
ubuntu:x:1001:1001:,,,:/home/ubuntu:/bin/bash
sshuser:x:1000:1000:,,,:/home/sshuser:/bin/bash
root@ubunu2004:/home/ubuntu# _
```

11. Podaj wnioski z wykonania powyższej części ćwiczenia.

Zakończ sesje.

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

Przykład korzystanie z SCP (Secure Copy).

1. ~Będąc zalogowanym do użytkownika ubuntu utwórz plik tekst.txt

```
ubuntu@ubunu2004:~$ touch test.txt
```

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

```
ubuntu@ubunu2004:~$ 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:tBAhyabVm526PiuKybuFfsoRou28q6QrRb8yAdVFf7U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
sshuser@10.0.0.30's password:
test.txt                                      100%    0     0.0KB/s   00:00
ubuntu@ubunu2004:~$ _
```

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

```
ubuntu@ubunu2004:~$ 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
ubuntu@ubunu2004:~$
```

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 (!ls -l).

```
ubuntu@ubunu2004:~$ 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/ubuntu
sftp> ls -l
-rw-rw-r--    1 sshuser  sshuser         0 Jan 12 18:09 test.txt
sftp> !ls -l
total 32
drwxr-xr-x 2 ubuntu ubuntu 4096 Apr 24  2020 Desktop
```

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

18. Usuń plik debian.txt na zdalnym serwerze.

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

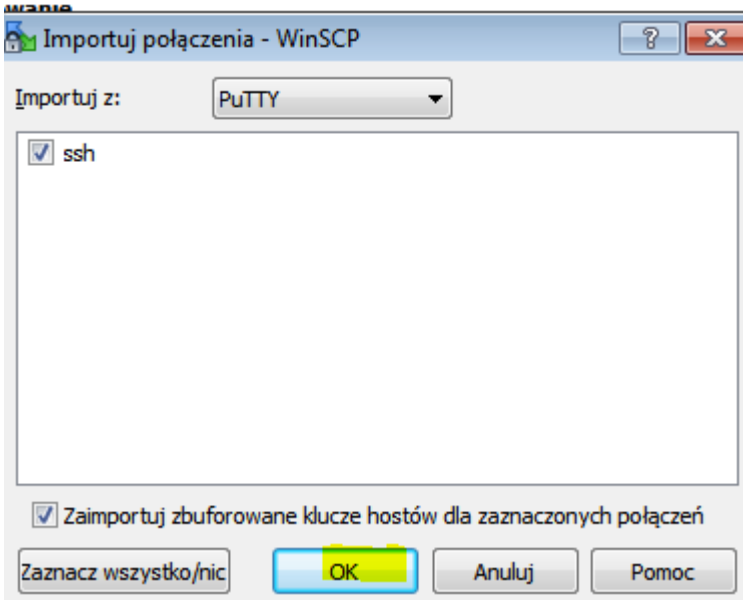
19. Zakończ połączenie z zdalnym serwerem.

```
sftp> quit
```

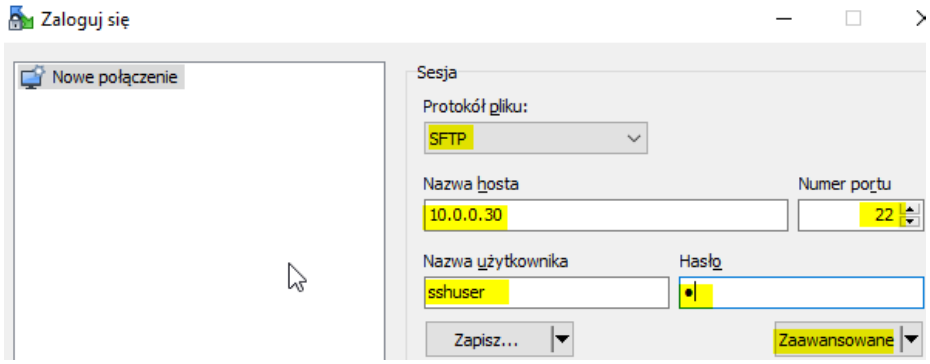
20. Podaj wnioski z wykonania powyższej części ćwiczenia.

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

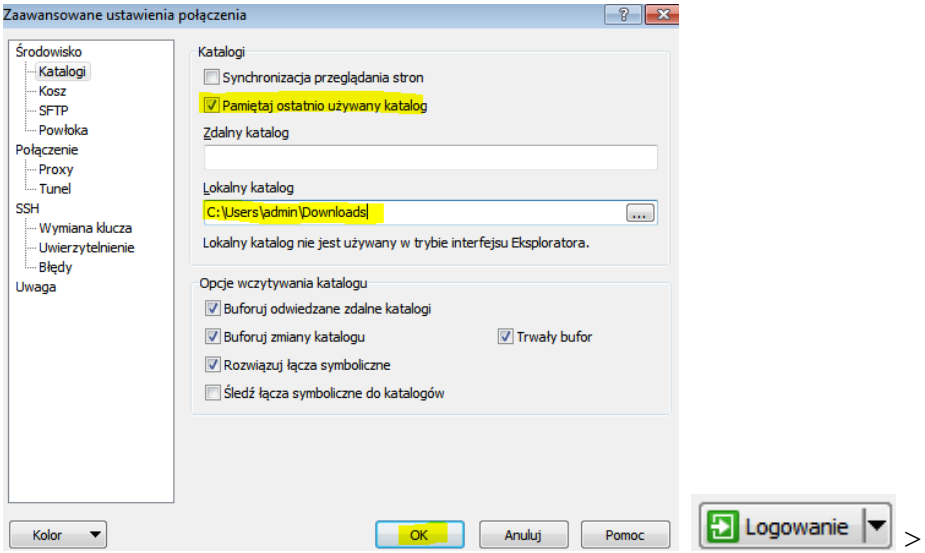
1. Pobierz, zainstaluj (typowa instalacja) i uruchom WinSCP, importuj połączenia



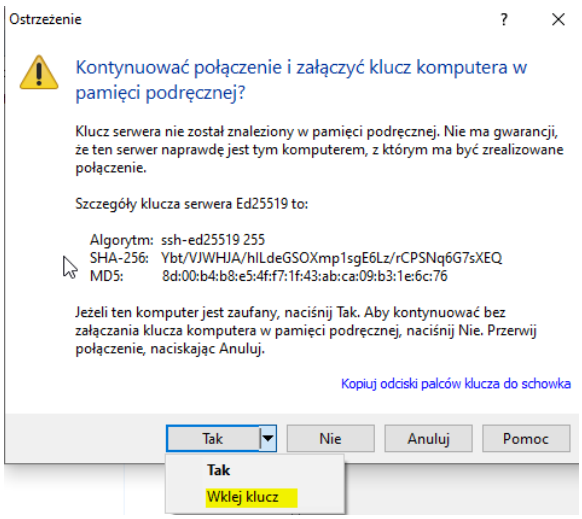
2. Jeżeli nie będzie ekranu jak poniżej kliknij przycisk "Nowy".
3. Na ekranie wyświetlane są informacje służce, aby się zalogować, uzupełnij je (wprowadź hasło logowania użytkownika), wybierz Zaawansowane.



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.

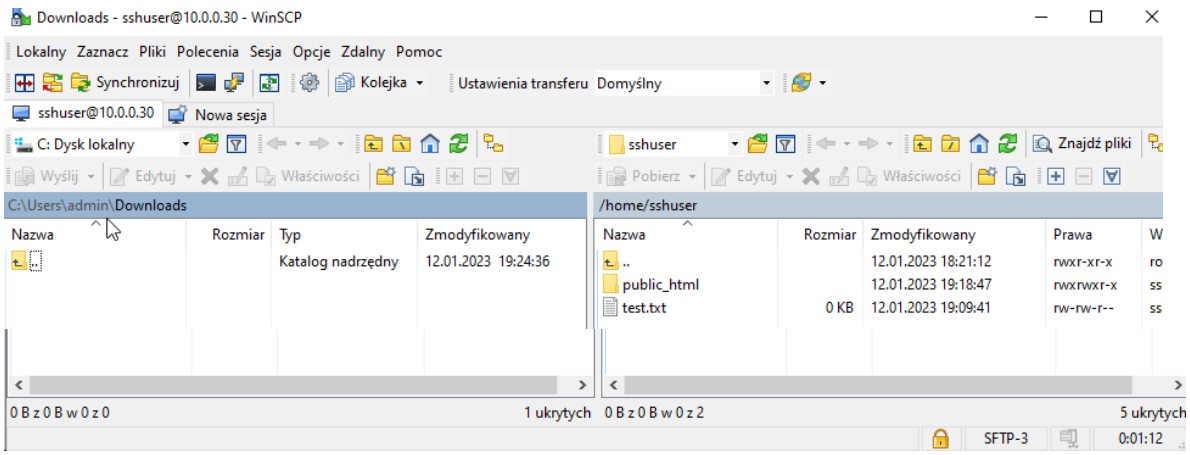


>



> ok

5. Po zalogowaniu możliwe jest przesyłanie i pobieranie plików.



6. Podaj wnioski z wykonania powyższej części 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@ubuntusrv:~# su ubuntu
ubuntu@ubuntusrv:/root$ 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:YlgKI8WzuPWkjPOqSm12rj2LnC5VtMEzHoIGEz4oZyI ubuntu@ubuntusrv
The key's randomart image is:
+---[RSA 3072]----+
|=oo .            |
|o=o. B           |
|E+=o+ B          |
|+=+o.B           |
| = ++ o S        |
|+ +... .         |
| +.+ .           |
|..= *.           |
|*.o*.+o          |
+----[SHA256]-----+
```

b) Zmień nazwę pliku i prawa do pliku.

```
ubuntu@ubuntusrv:/root$ mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
ubuntu@ubuntusrv:/root$ 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@ubunu2004:/home/ubuntu# adduser ucze
New password:
Retype new password:
root@ubunu2004:/home/ubuntu# su ucze
ucze@ubunu2004:/home/ubuntu$ mkdir ~/.ssh
ucze@ubunu2004:/home/ubuntu$ chmod 700 ~/.ssh
```

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

```
ucze@ubunu2004:/home/ubuntu$ 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:tBAhyabVm526PiuKybuFfsoRou28q6QrRb8yAdVFf7U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
ubuntu@10.0.0.30's password:
id_rsa                                        100% 2602     2.5MB/s   00:00
```

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

```
ucze@ubunu2004:/home/ubuntu$ ssh ubuntu@10.0.0.30
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)
ubuntu@ubuntusrv:~$ _
```

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

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

```
root@ubuntusrv:/home/ubuntu# nano /etc/ssh/sshd_config
```

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

8. Zrestartuj usługę ssh

systemctl restart ssh

```
root@ubuntusrv:/home/ubuntu# systemctl restart ssh
```

9. Podaj wnioski z wykonania powyższej części ćwiczenia.

następnie zakończ sesje i wyłącz ubuntu desktop

```
root@ubuntusrv:/home/ubuntu# exit
exit
ubuntu@ubuntusrv:~$ exit
logout
Connection to 10.0.0.30 closed.
ucze@ubunu2004:/home/ubuntu$ init 0
```

```
ucze@ubunu2004:/home/ubuntu$ systemctl poweroff -i
```

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.

```
root@ubuntusrv:/home/ubuntu# nano /etc/ssh/sshd_config
```

```
#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` lub

```
root@ubuntusrv:/home/ubuntu# systemctl restart ssh
```

2. Z klienta Windows zaloguj się do serwera SSH.

```
ubuntu@ubuntusrv: ~
login as: ubuntu
ubuntu@10.0.0.30's password:
Welcome to Ubuntu 20.04 LTS (GNU/
```

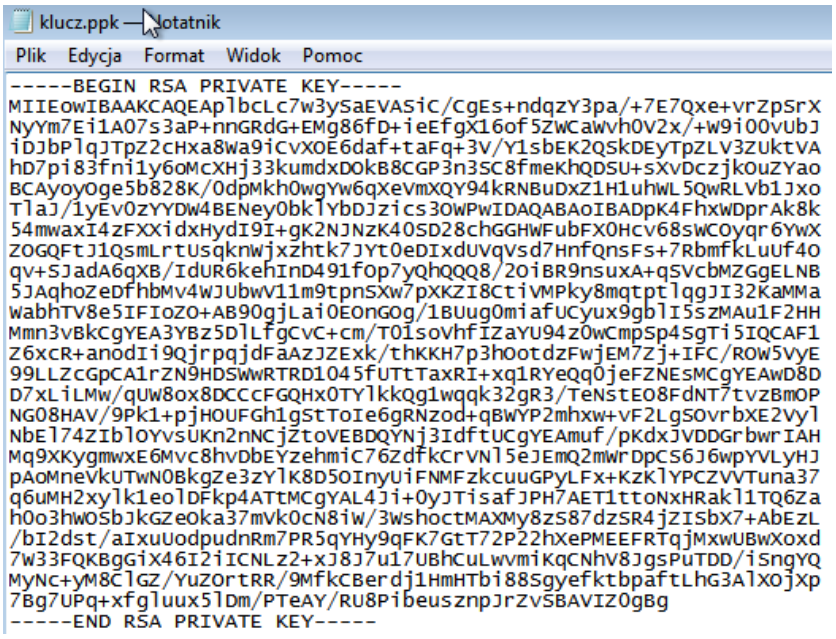
a) edytuj plik id_rsa,

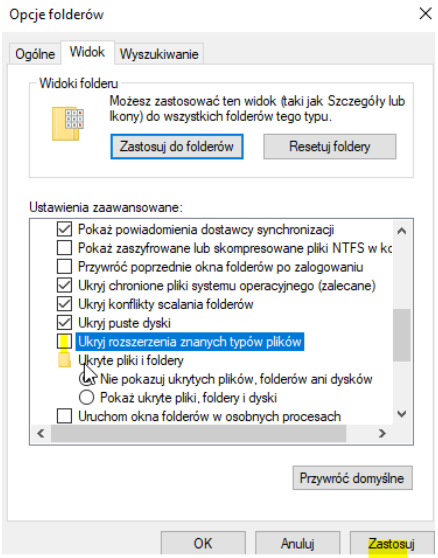
nano /home/ubuntu/.ssh/id_rsa

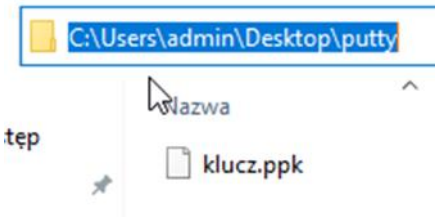
```
ubuntu@ubuntusrv:~$ nano /home/ubuntu/.ssh/id_rsa
```

```
ubuntu@ubuntusrv: ~
  GNU nano 4.8                                    /home/ubuntu/.ssh/id
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAwl+ZVFP63RHNlO/imSWGMpnvISrglwkshHh6gSt9xuopa+/rbPaw
n6IlrZbj7mydOtlDt9uoFn6FueM/bIHlc0d5Nudo2rGZeZOXoz+NryJQ4rmJtieP9BGmMZ
2xMzmSTzerl6MB0WdEru0JMjjml00FOf4o0ohjrKEvMCEIGES0dR2gOWfTyXPQSbFOp0JG
NVfGhS/i5kI8/okINiTl3NNUMV5oY4S3qdK3DtMqNpDx56lJJM42G5qsIOW4b/YbKiynD2
32V5cHatZgZKZ4FrPKY+WwKlSUAr3jvlKa6cGY/+EIVQ5zXIqoJco4T8K9q7Rl+LtakT2N
Wl/ObAgc/OExFSKEvYHH3tUjr04KKvZvto9yaQ4qTspSItwuqS96MlNNTMyvoOnxNhCXqF
YFPVGQ+lCf9WvxRsp2gi4K0JysIrXhj/jxl7oD8sE3k7cyHMnetXYd2sDXU8TsHkAVVgm/
v9mhub2nvBKE31AOA4S0WA7FZ5Pi0/5AiMD6Ym4vAAAFiPl9iOD5fYjgAAAAB3NzaClyc2
EAAAGBAMNfmVRT+t0RzZTv4pklhjKZ7yEq4NcJLIR4eoErfcbqKWvv62z2sJ+iJa2W4+5s
nTrdQ7fbqBZ+hbnjP2yB9XNHeTbnaNqxmXmTl6M/ja8iUOK5ibYnj/QRpjGdsTM5kk83q9
ejAdFnRK7tCTI45pdNBTn+KNKIY6yhLzAhCBhEtHUdoDln08lz0EmxTqdCRjVXxoUv4uZC
PP6JCDYk9dzTVDFeaGOEt6nStw7TKjaQ8eetSSTONhuarCDluG/2Gyospw9t9leXB2rWYG
SmeBazymPlsCpUlAK9475SmunBmP/hCFUOclyKqCXKOE/Cvau0Zfi7WpE9jVtfzmwIHPzh
MRUihL2Bx97VI69OCir2b7aPcmkOKk7KUiLcLqkvejJTTUzMr6Dp8TYQl6hWBTlRkPpQn/
Vr8UbKdoIuCtCcrCK14Y/48de6A/LBN5O3MhzJ3rV2HdrAllPE7B5AFVYJv7/Zobm9p7wS
hN9QDgOEtFgOxWeT4tP+QIjA+mJuLwAAAAMBAAEAAAGBAKDd9Fg1FdglMnsx0fibpxW/He
DHd35XtWoV8XiuINBKOnT/hW+g5+lpD3ERTvggQo4XZgzbNlnfL6jRboWftESJU0tb20BG
/8HVPwRR7g2ISeWFM9jiVmt2pMsxtpghDVFg240gWnzbdPg7gFjz9RobdvQ7S82eM8QOq9
YLPKkO2S+dhzH9RasYSyaCcerSbRC7B2De/wrs+l/x4OsEH9UFxMspmvZmbvvL3qK8SIPJ
cQV77z/48yBjiNtFi0nU7zQvrnQgwwHywS9XAJ+72vApFEHNT96oYgytv9ufY73LSMECVt
7sBhq3gq2cFQhS8LZtS0hAZaUHN0FC6tXHHEQ7s8IhJMV3xZGUruB2t6kLItS3WOzCbop3
yU0gXValoJjQFL0xHpMcbE8L6iMA7U7lnzNPwQ7n/BUJTKzn4tC48FK/BewSUFxLdWQNFD
nb3qy2BXPVlyHLJ3F9XCE6dylFbJUl53M9eJgLrcpCOJekxqfvmpioRCY2qCc7DIF28QAA
AMBbItjMlMI90jAjm7jVdLRpjXsHZlHGlCfk6nXLD9Yo7mFd7td16pER7b+3o5YONO7fny
aTK9lUqvUf0iL9qpENyy+XCHrEPQZSRB5gsXVekODqaVPFNPrWKieIgnRCFhQCVDd4Y63/
txnyLlanS/6egAQJrekFPGbdP2u+o557J7SKANq9t+LlVOBlrRXjW0912K/0+BZvxQGpxH
/OIDxZJKjRvoj3G98tQI7uwUs/s3ZVkGSSfvy4TGTSHisUmlkAAADBAOz+molR993okEVQ
HlD4fiNzUurt/HSRLLWJGRzT4VHzqniGk90SFJSjQ+GiJEpnyu9wss9JiKLPfymsB8KRsg
eyWwnbEXR7lLroKQIGwy/una75bJCpMcVb2+tj23q56f2p3oPcrhqxPouUgi4V2Y5hQlF/
3myupxykA7MfYGrZgCdRYWs7w5ry4RtuGAnoSw2nfBcCOTxwHv5gO0m+Ni9kGMadsi88kl
lW5xLRvK7ZSFhx0Z09FkIjUCj5TB0ZWwAAAMEA0wqIHhW8Z+lLzeGl8hu0J7l/6a3xTqns
qX+c0zKTdsVyXYPODzQvKALhuQwMEWLpzl+iZgJQ0blhbnauapqRRiexCoGbxLB3TdCRyh
FCtkj56LhfJbdqsbAtiHZn9wZbG56PuzMICqSZmctByGsmiCWNli7smQaP42ZhjIOgoZln
atWHoktvPObusk8ldsZGepDALq+ApyW+CGvsKo/ksXwJsfTul8zEeB4uH5wRiuDi30uR4X
7dH9KduSv2XAK9AAAAEHVidW50dUBlYnVudHVzcnYBAg==
-----END OPENSSH PRIVATE KEY-----
```

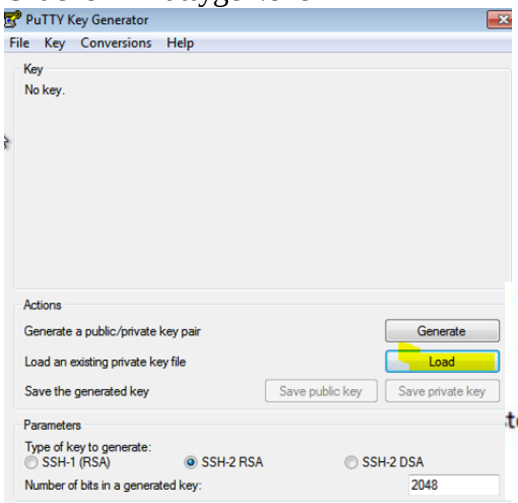
b) przekopiuj zawartość id_rsa do nowo utworzonego w Windows (Desktop\putty) pliku klucz.ppk.

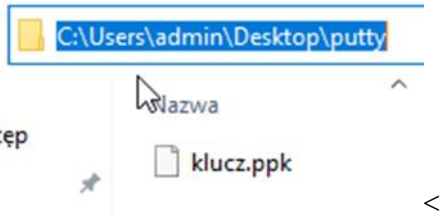




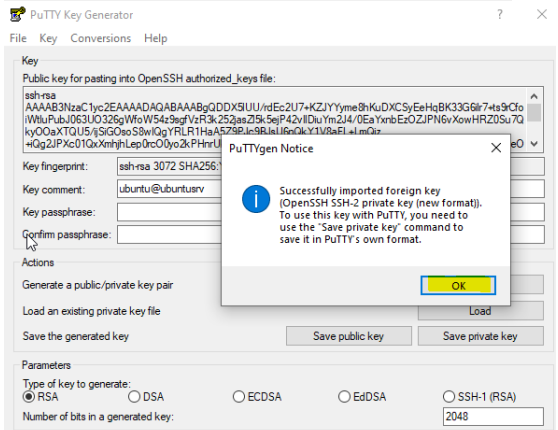


c) Uruchom "Puttygen.exe" z materiałów i kliknij przycisk "Load".

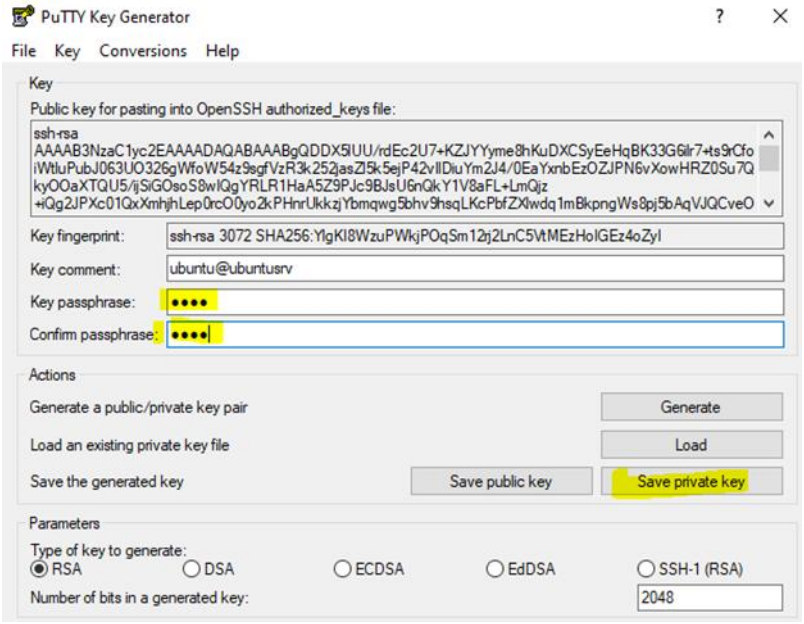




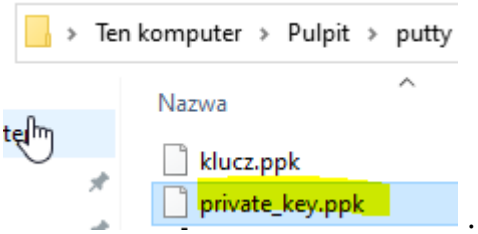
< wybierz ten klucz



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

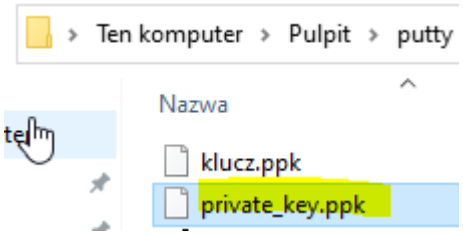


e) Kliknij "Save private key", aby zapisać je w folderze z dowolną nazwą pliku np.

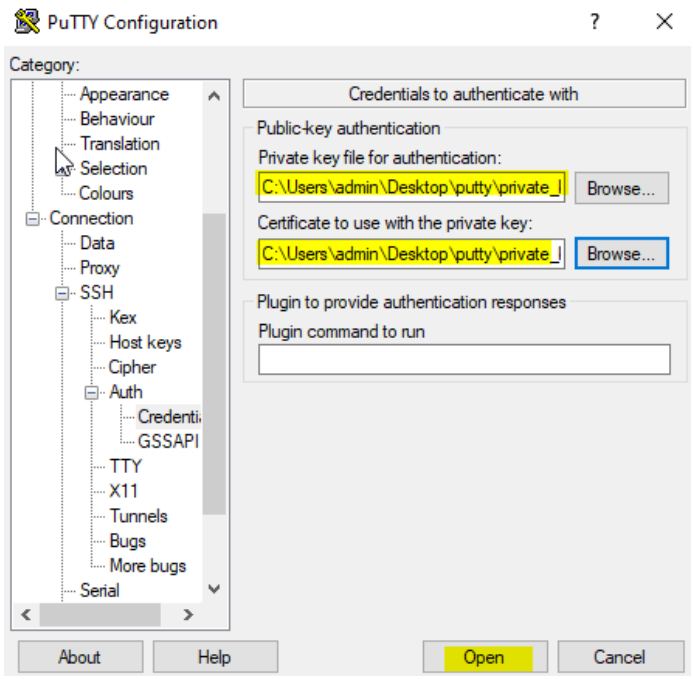


Nie generuj klucza. Nie zmieniaj wartości "Number of bits In a generated key".

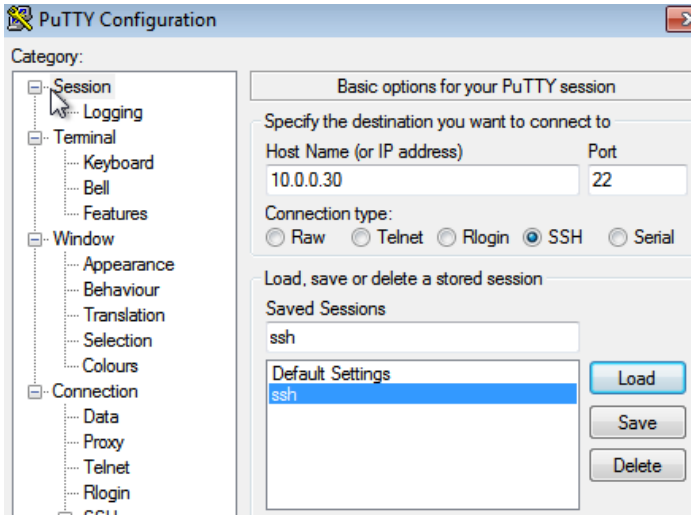
Podczas generowania certyfikatów ustawienie jak na zrzucie poniżej powoduje długi czas tworzenia certyfikatów.



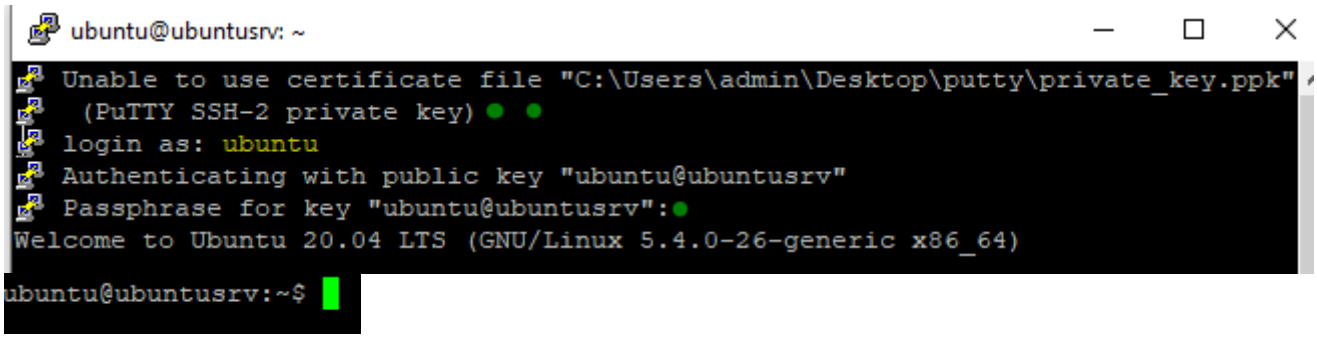
3. Uruchom putty i otwórz [Połączenie] - [SSH] - [Auth] w menu po lewej stronie, a następnie wybierz "private_key", który został właśnie zapisany powyżej.



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



5. Hasło jest wymagane, podaj login ubuntu a następnie tajny klucz - hasło: 4321 jest ono odebrane i sprawdzane. Jeśli hasło jest poprawne, to zalogowanie jest możliwe.

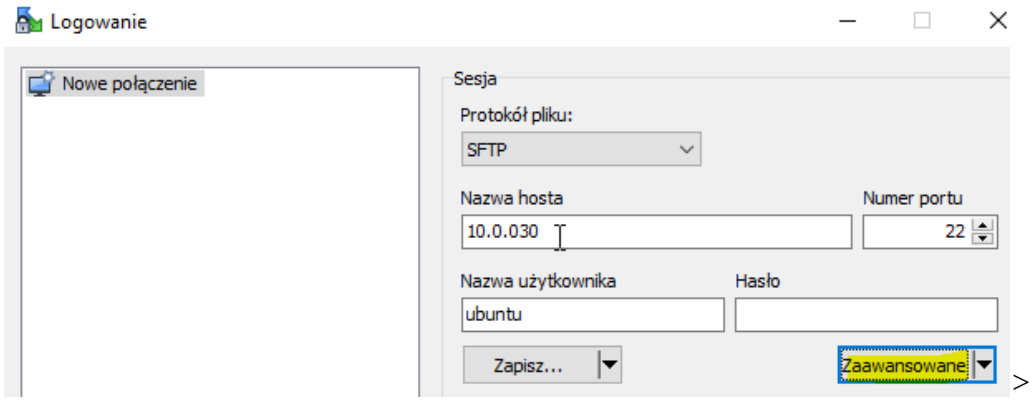


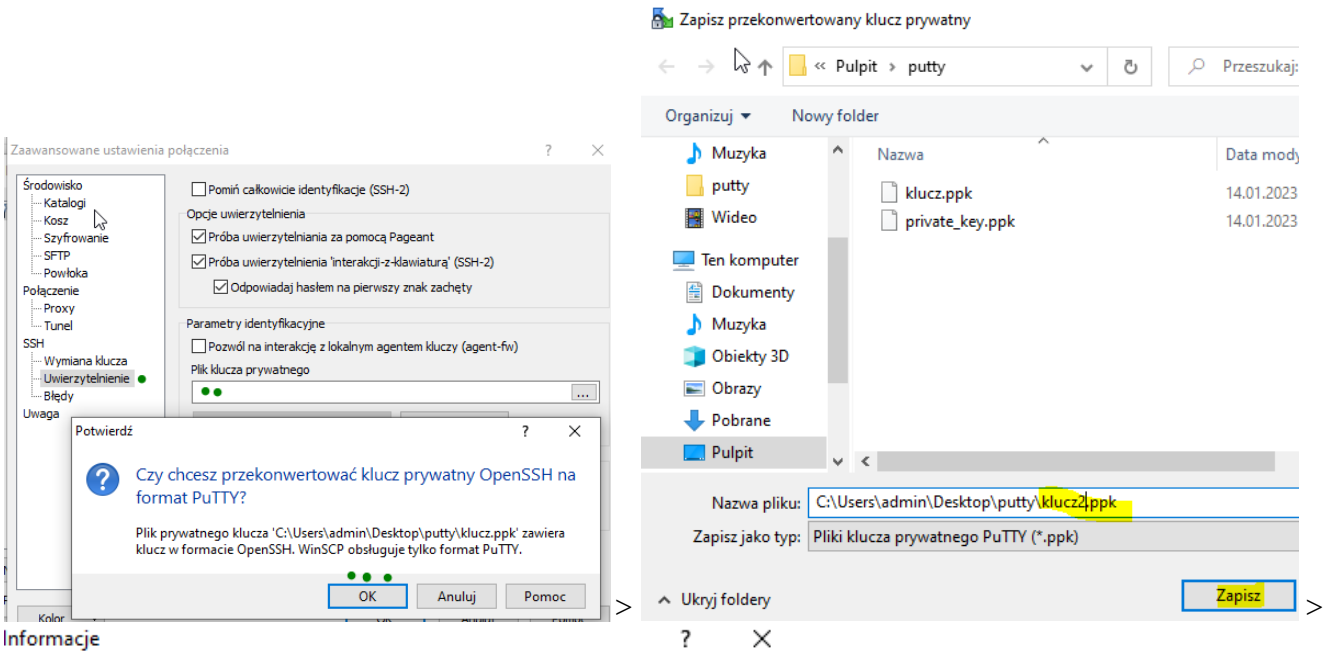
6. Pokaż aktualny katalog na zdalnym serwerze (pwd).
7. Pokaż pliki w bieżącym katalogu na serwerze FTP (ls -la).

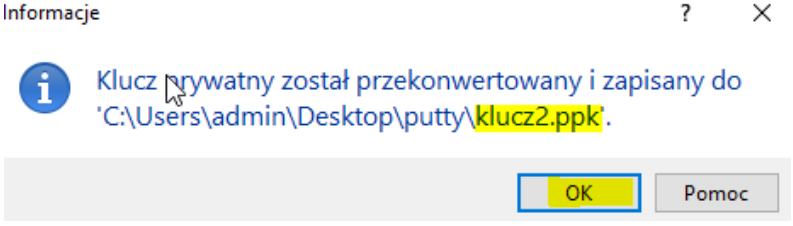
```
ubuntu@ubuntusrv:~$ pwd
/home/ubuntu
ubuntu@ubuntusrv:~$ ls -la
total 36
drwxr-xr-x 5 ubuntu ubuntu 4096 Jan 14 14:44 .
drwxr-xr-x 4 root   root   4096 Jan 14 12:06 ..
-rw------- 1 ubuntu ubuntu  194 Jan 14 14:35 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Apr 26  2021 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Apr 26  2021 .bashrc
drwx------ 2 ubuntu ubuntu 4096 Apr 26  2021 .cache
drwxrwxr-x 3 ubuntu ubuntu 4096 Jan 14 14:44 .local
-rw-r--r-- 1 ubuntu ubuntu  807 Apr 26  2021 .profile
drwx------ 2 ubuntu ubuntu 4096 Jan 14 14:44 .ssh
-rw-r--r-- 1 ubuntu ubuntu    0 Apr 26  2021 .sudo_as_admin_successful
```

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

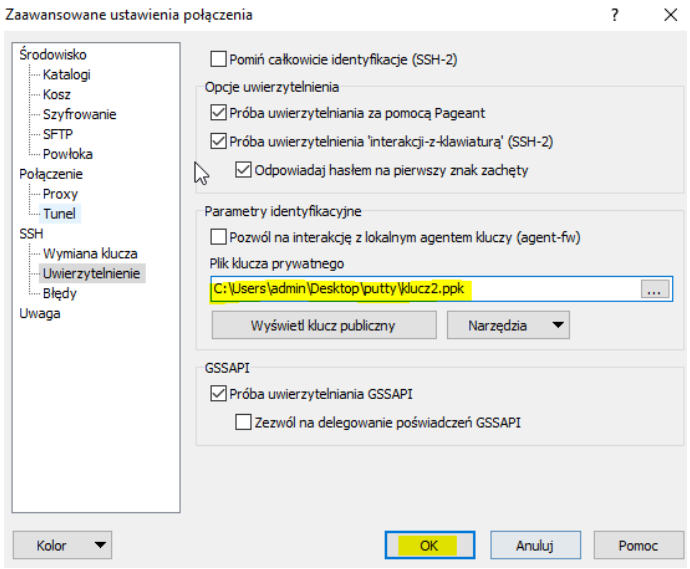
a) Ustaw parametry sesji i użytkownika.



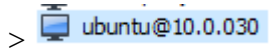




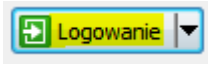
b) Podłącz plik klucza prywatnego.



c) Zapisz sesję jak poniżej.



d) Zaloguj się (połącz się z serwerem ubuntu@10.0.0.30).

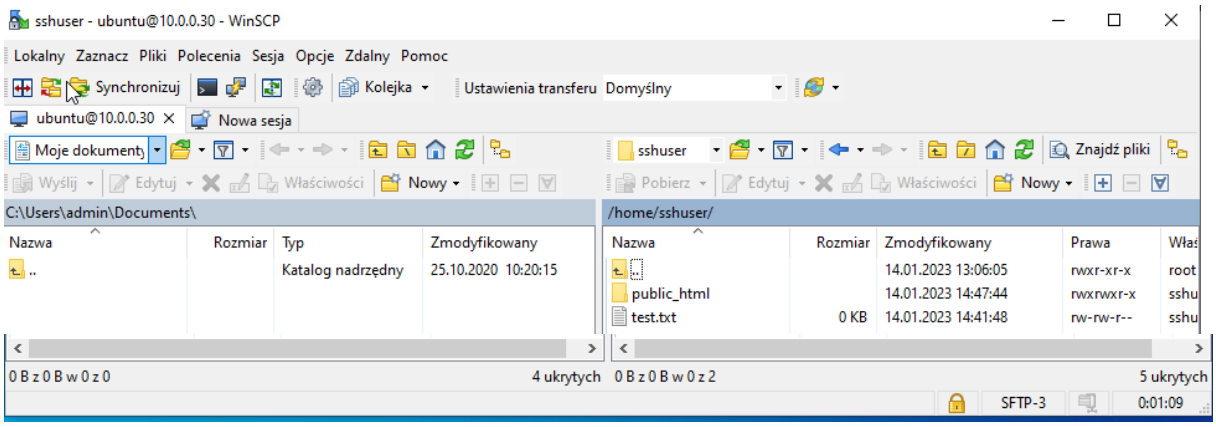


9. Wprowadź hasło dla klucza.

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

Jeśli hasło jest poprawne, to zalogowanie jest możliwe.

b) Efekt końcowy.



10. Podaj wnioski z wykonania powyższej części ćwiczenia.

Jeśli twój Windows to Windows 10 w wersji 1803 lub wyżej, 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.

Przywróć pierwszą migawkę

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.