## 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.

Ubuntu serwer Adapter 1	Ubuntu serwer Adapter 2
Sieć Karta 1 Karta 2 Karta 3 Włącz kartę sieciową Podłączona do: NAT Nazwa: Zaawansowane	Sieć Karta 1 Karta 2 Karta 3 Karta 4 Włącz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: intnet Zaawansowane
Windows Adapter 1	Ubuntu desktop Adapter 1
Sieć Karta 1 Karta 2 Karta 3 Karta 4 Włącz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: intnet	Sieć Karta 1 Karta 2 Karta 3 Włącz kartę sieciową Podłączona do: NAT Nazwa: Zaawansowane

Po uruchomieniu Ubuntu podaj login: ubuntu Password: ubuntu

Wisz sudo -s Password: ubuntu

Ustawienie statycznego adresu IP

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Za pomoca polecenia ifconfig -a ustal dostępne interfejsy sieciowe.

root@dlp:~# ifconfig -a
enp0s3: flags=4163 <up,broadcast,running,multicast> mtu 1500</up,broadcast,running,multicast>
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< td=""></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</up,broadcast,running,multicast>

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 c	onfig written by 'subiquity'
network:	
version: 2	
renderer: networkd	
ethernets:	
enpOs17:	
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 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 usługe ssh



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:	~# net	tstat -	ant   grep 22		
tcp	0	00	).0.0.0: <mark>22</mark>	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 protokółu 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

telnetissh.iso

3. Korzystając z Putty skonfiguruj sesje ssh.



4. Otwórz sesje ssh.

PuTTY Sec	urity Alert
<u>^</u>	The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's rsa2 key fingerprint is: ssh-rsa 2048 3d:74:9c:2d:d2:a9:34:05:bb:7c:74:a9:eb:1f:2e:54 If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon the connection.
	Tak Nie Anuluj

5. Zaloguj się jako użytkownik sshuser z hasłem.



Zakończ sesje exit.

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



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_conf ig
#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 # <mark>PermitRootLogin prohibit-password</mark> #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 zmień opcję umożliwiającą zalogowanie jako root jak poniżej.

PermitRootLogin no

Wykonaj systemctl restart ssh

3. Przejdź na Windows. Otwórz sesje ssh, wykonaj próbę zalogowania się jako użytkownik root

z hasłem. Korzystając z su przejdź do użytkownika root.



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	Urz	adzer	nia	Pomo	c
root	@bolek-\	/irtual8	3ox:~#	apt	-y	ins	tall	openssh-client
					Sioć			



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:~<mark># netplan apply</mark>

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 (10.0.30)' can't be established.
ECDSA key fingerprint is SHA256:I2/syI68V386KQTcsZ1HpUqMfwNFM8+m6K60jafW13E
Are you sure you want to continue connecting (yes/no)? <mark>yes</mark>
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
                                     IP address for enp0s3: 10.0.2.15
  Memory usage: 16%
                                     IP address for enp0s8: 10.0.0.30
  Swap usage:
                 0%
67 packages can be updated.
37 updates are security updates.
Last login: Sun Sep 30 22:07:42 2018
ubuntu@dlp:~$ _
```

4. Zakończ sesje 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 https://landscape.canonical.com \* Management: \* Support: https://ubuntu.com/advantage System information as of Mon Oct 1 00:01:28 CEST 2018 System load: 0.04 Processes: 101 0.2% of 914.76GB Users logged in: Usage of /: 2 Memory usage: 16% IP address for enp0s3: 10.0.2.15 Swap usage: IP address for enp0s8: 10.0.0.30 0% 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	:~# ne	tstat -ant I	grep 22		
tcp	0	0 0.0.0.0	): <mark>22</mark>	0.0.0:*	LISTEN
tcp	0	0 10.0.0	. 30 : <mark>22</mark>	10.0.0.53:53110	ESTABL ISHED
tcp	0	0 10.0.0	. 30 : <mark>22</mark>	10.0.0.51:49167	ES TABL ISHED
tcp6	Θ	0 ::: <mark>22</mark>		:::*	LISTEN

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

root@bolek–VirtualBox:~# ssh ubuntu@10.0.0.30 "cat /e	tc∕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	
Sandaci (A. 1002, 1002, , , , Andilley Sandaci (Abiti/ busi)	

Podaj wnioski z wykonania powyższego ćwiczenia.

Zakończ sesje.

# 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:~\$ <mark>scp ./test.txt sshuser@10.0.0.30:~/</mark> The authenticity of host '10.0.0.30 (10.0.0.30)' can't be establis ECDSA key fingerprint is SHA256:I2/syI68V386KQTcsZlHpUqMfwNFM8+m6K Are you sure you want to continue connecting (yes/no)? <mark>yes</mark> Warning: Permanently added '10.0.0.30' (ECDSA) to the list of know	shed. 60jafW13 wn hosts.	3E.		
sshuser@10.0.0.30's password: Permission denied, please try again. sshuser@10.0.0.30's password: ● test.txt bolek@bolek-VirtualBox:~\$ _	100%	0	0.0KB/s	00:00

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

polek@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 -!).



- 9. Utwórz katalog public html
- 10. Przejdź do katalogu public\_html
- 11. Pokaż aktualny katalog na zdalnym serwerze (pwd).



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

sftp> <mark>put t</mark>	test.txt_ubunt	tuserv.txt						
Uploading t	test.txt to /ł	nome/sshuser/	′public_html	/ubuntuserv.	txt			
test.txt					100%	0	0.0KB/s	00:00
sftp≻ ls −l	L							
-rw-rw-r	1 sshuser	sshuser	0 Oct	1 00:19 ubu	ntuserv.txt			

13. Prześlij jakiś plik txt do zdalnego serwera.

sftp> <mark>put *.</mark>	txt							
Uploading te	st.txt to /h	nome/sshuse	r∕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 t	test.txt			
-rw-rw-r	1 sshuser	sshuser	0 Oct	1 00:19 ι	ubuntuserv.txt			

14. Pobierz plik test.txt z zdalnego serwera.

sftp> <mark>get test.txt</mark> 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> <mark>mkdir</mark> sftp> ls −l	testdir						
-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 sftp> ls –l	testdir						
-rw-rw-r	1 sshuser	sshuser	0	Oct	1	00:20	test.txt
-rw-rw-r	1 ssnuser	ssnuser	V	UCT	1	00:19	upuntuserv.txt

18. Usuń plik debian.txt na zdalnym serwerze.

```
sftp> <mark>rm ubuntuserv.txt</mark>
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 bolek@bolek-VirtualBox:<sup>~\$</sup> 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

🌆 Importuj po	łączenia -	- WinSCP		? <mark>×</mark>
Importuj z:	PuTT	γ	•	
🔽 ssh				
<b>V</b> Zaimportuj	zbuforowa	ane klucze hostó	ów dla zaznaczo	nych połączeń
Zaznacz wszyst	ko/nic	ОК	Anuluj	Pomoc

- 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.

🊰 Zaloguj się		
Nowe połączenie	Sesja Protokół <u>pliku:</u> SFTP Nazwa <u>h</u> osta 10.0.0.30	Numer portu
	Nazwa <u>u</u> żytkownika Hasł <u>o</u> sshuser • Zapisz V Anuluj	Z <mark>aawansowan</mark> e 💌

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.

🌆 sshuser - ssh - WinSCP									
Lokalny Zaznacz Pliki P	olecenia Seș	ja Opcje Zdalny Po	moc						
🖶 🚼 📚 Synchronizuj	🖶 🚼 📮 Synchronizuj 🔲 🐙 💽 🍈 🎒 Kolejka 👻 Ustawienia transferu Domyślny 🔹 🥩 🗸								
📮 ssh 💣 Nowa sesja									
🚢 C: 🍢 ysk loka 🔻 🚰 🝸	<b> </b> ← + →	- 🗈 🖬 🏠	2	📔 ssi 🔹 🚰 🔽 🖛 🗸	-> - 主	🔁 🏠 🔁 🗖			
🛃 Wyślij 👻 📝 Edytuj	• × 🛃 🗈	Właściwości 🌺 🛛	+ »	Pobierz 👻 📝 Edytu	j <b>- X</b> 🚮 🛛	Właściwości 🎽 🕂 🎽			
C:\Users\admin\Downloads				/home/sshuser					
Nazwa	Rozmiar	Тур	Zm	Nazwa	Rozmiar	Zmodyfikowany			
<b>a</b>		Katalog nadrzędny	201	Left for the second sec	0 KB	2018-09-30 23:27:33 2018-10-01 00:24:55 2018-10-01 00:09:28			
•			÷.	۰ III		•			
0 B z 0 B w 0 z 0		1 ukŋ	/tych	0 B z 0 B w 0 z 2	0	6 ukrytych			
					SFT	P-3 📃 0:00:28			

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.

11 U
root@dlp:~# <mark>su ubuntu</mark>
ubuntu@dlp:~\$ 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:DS30i6xhY1N6t2J9m8d2hL3hAE9EVZjsgrIkadWsnOk_ubuntu@d1p
The key's randomart image is:
+[RSA 2048]+
I .o .o.+ol
Ioo .+ I
l +++o l
I ++B=.o I
I .B+So+ +. o I
l o *Eo.ool
l . o oo.ol
I o+o.l
l oo.l
+[SHA256]+

b) Zmień nazwę pliku i prawa do pliku.

```
ubuntu@dlp:~$ mv ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
ubuntu@dlp:~$ 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#	addusen 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).

```
The authenticity of host '10.0.0.30 (10.0.0.30:/home/ubuntu/.ssh/id_rsa ~/.ssh

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
                   https://landscape.canonical.com
 * Management:
 * Support:
                   https://ubuntu.com/advantage
  System information as of Mon Oct 1 00:58:16 CEST 2018
  System load:
                0.01
                                   Processes:
                                                           98
                0.2% of 914.76GB
  Usage of /:
                                   Users logged in:
                                                           1
  Memory usage: 16%
                                   IP address for enp0s3: 10.0.2.15
                                   IP address for enp0s8: 10.0.0.30
  Swap usage:
                0%
67 packages can be updated.
37 updates are security updates.
_ast login: Mon Oct _1 00:01:29 2018 from 10.0.0.53
ubuntu@dlp:~$
```

7. W wierszu 56 ustaw "PasswordAuthentication nie", 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

<b>ه 192</b>	167.0.1 -	PuTTY							
GNÜ	nano	2.2.6		Plik:	/home/	sshuser	/.ssh/i	d_rsa	
F	BEGIN	RSA P	RIVATE	KEY					
MIIEou	WIBAAN	KCAQEA	plbcLc7	w3ySaEV	/ASiC/C	gEs+ndq	zY3pa/+	7E7Qxe+	vrZpSrX
NyYm7I	Ei1A07	7s3aP+	nnGRdG+	EMg86fI	)+ieEfg	X16of5Z	WCaWvh0	V2 <b>x/+</b> W9	i00vUbJ
iDJbP]	lqJTp2	Z2cHxa	8Wa9iCv	XOE6dai	f+taFq+	3V/Y1sb	EK2QSkD	EyTpZLV	3ZUktVA
hD7pi8	B3fni1	ly6oMc	XHj33ku	mdxDOkE	38CGP3n	3SC8fme	KhQDSU+	sXvDczj	kOuZYao
BCAyoy	yOge51	0828K/	0dpMkh0	wgYw6qX	KeVmXQY	94kRNBu	DxZ1H1u	hWL5QwR	LVb1Jxo
TlaJ/1	lyEv02	zYYDW4	BENey0b	klYbDJ2	zics30W	PwidaQa	BAoIBAD	pK4FhxW	DprAk8k
54mwa	xI4zFX	KXidxH	ydI9I+g	K2NJNzB	40SD28	chGGHWF	ubFX0Hc	v68sWCC	yqr6YwX
ZOGQF1	tJ1Qsr	nLrtUs	qknWjxz	htk7JYt	t0eDIxd	UVqVsd7	HnfQnsF	s+7Rbmf	kLuUf40
qv+SJa	adA6qX	KB/IdU	R6kehIn	D491fOp	o7yQhQQ	Q8/20iB	R9nsuxA	+qSVcbM	ZGgELNB
5JAqho	oZeDfh	nbMv4W	JUbwV11	m9tpnS)	W7pXKZ	18CtiVM	Pky8mqt	ptlqgJI	32KaMMa
WabhT	V8e5IH	FIoZO+	AB90gjL	ai0EOn0	GOg/1BU	ug0miaf	UCyux9g	blI5szM	Au1F2HH
Mmn 3vI	BkCgYE	EA3YBz	5D1LfgC	vC+cm/1	[01soVh	fIZaYU9	4z0wCmp	Sp4SgTi	5IQCAF1
Z6xcR-	+anod]	[i9Qjr	pqjdFaA	zJZExk/	thKKH7	p3h0otd	zFwjEM7	Zj+IFC/	ROW5VyE
99LLZ	GpCA1	lrZN9H	DSWwRTR	D1045fU	JTtTaxR	I+xq1RY	eQq0jeF	ZNEsMCg	YEAwD8D
D7xLi	LMw/ql	JW8ox8	DCCcFGQ	Hx0TY13	ckQg1wq	q <mark>k</mark> 32gR3	/TeNstE	O8FdNT7	tvzBmOP
NG08H	AV/9P)	k1+pjH	OUFGh1g	StTole	5gRNzod	+qBWYP2	mhxw+vF	2LgSOvr	bXE2Vyl
NbE174	4ZIbl(	OYvsUK	n2nNCjZ	toVEBDÇ	QYNj3Id	ftUCgYE.	Amuf/pK	dxJVDDG	rbwrIAH
Mq9XK	ygmwxI	E6Mvc8	hvDbEYz	ehmiC76	5ZdfkCr	VN15eJE	mQ2mWrD	pCS6J6w	pYVLyHJ

AoMneVkUTwN0Bkg2e3zY1K8D50InyUiFNMFzkcuuGPyLFx+KzKlYPC2VVTuna37 q6uMH2xylk1eolDFkp4ATtMCgYAL4Ji+0yJTisafJPH7AET1ttoNxHRakl1TQ6Za h0o3hWOSbJkGZeOka37mVk0cN8iW/3WshoctMAXMy8zS87dzSR4jZISbX7+AbEzL /bI2dst/aIxuUodpudnRm7PR5qYHy9qFK7GtT72P22hXePMEEFRTqjMxwUBwXoxd 7W33FQKBgGiX46I2iICNLz2+xJ8J7u17UBhCuLwvmiKqCNhV8JgsPuTDD/iSngYQ MyNc+yM8ClGZ/YuZOrtRR/9MfkCBerdj1HmHTbi88SgyefktbpaftLhG3AlXOjXp 7Bg7UPq+xfgluux51Dm/PTeAY/RU8PibeusznpJrZvSBAVIZ0gBg -----END\_RSA\_PRIVATE\_KEY-----

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

🔄 klucz.ppk — Notatnik			
Plik Edycja Format Widok Pomoc			
BEGIN RSA PRIVATE KEY MIIEOWIBAAKCAQEAplbcLc7w3ySaEVASiC/CgEs+ndqzY3pa/+7E7Qxe+vrZpSrX NyYm7Ei1A07s3aP+nnGRdG+EMg86fD+ieEfgX16of5ZWCaWvhOV2x/+W9i00vUb iDJbPlqJTpZ2CHxa8wa9iCvXOE6daf+taFq+3V/YlsbEK2QSkDEyTpZLV3ZUktVA hD7pi83fni1y60MCXHj33kumdxD0kB8CGP3n3SC8fmeKhQDSU+sXvDczjk0uZYa0 BCAyoyOge5b828K/0dpMkh0wgYw6qxeVmXQY94kRNBuDX21H1uhwL5QwRLVb1Jx0 TlaJ/1yEv0ZYYDW4BENeyObklYbDJzics30WPWIDAQABA0IBADpK4FhxwDprAk8k S4mwax14zFXXidXHydI9I+gK2NJXzK40SD28chGGHWFubFX0Hcv68sWCOyqr67wX ZOGQFtJ1QsmLrtUsqknwjxzhtk7JYt0eDIxdUVqVsd7HnfQnsFs+7RbmfkLuUf40 qv+5JadA6qX8/IdUR6kehInD491f0p7yQhQQ8/20iBR9nsuXA+qSvCbMZGGELNB SJAqhoZeDfhbMv4WJUbWV11m9tpnSXW7pXKZI8CtiVMPky8mqtpt1qJI32KaMMa wabhTv8e5IFIoZ0+AB90gjLai0EonGog/IBUug0miafUCyux9gb1I5szMAuIF2HH Mmn3vBkCgYEA3YBZ5D1LfgCvc+cm/T01s0vhfIZaYU94z0wCmpSp4SgTi5IQCAF1 Z6xCR+anodIi9QjrpqjdFaAzJZExk/thKKH7p3hootdzFwjEMZZj+IFC/R0WSVyE 99LLZCGPCA1rZN9HDSWWRTRD1045fUTTaXRI+xq1RYeQQjEFZNESMCgYEAWB8D D7xLiLMw/qUW80x8DCCcFGQHx0TY1kkQq1wg432qR3/TeNstE08FdNT7tvzBmOP			
NG08HAV/9Pk1+pjHOUFGh1gStToIe6gRNzod+qBwYP2mhxw+vF2LgSOvrbXE2Vy1 NbE174ZIb1OYvsUKn2nNCjZtoVEBDQYNj3IdftUCgYEAmuf/pKdxJVDDGrbwrIAH Mq9XKygmwxE6Mvc8hvDbEYzehmiC76ZdfkCrVN15eJEmQ2mWrDpCS6J6wpYVLyHJ		▼ B C:\Users\ac	lmin\ <mark>Desktop\putty</mark>
pAOMnevkuTWNUBKgZe3ZYTK8D50INyUTFNMFZkCUUGPyLFX+KZKTYPCZVVTuna3/ q6uMH2xylk1eolDFkp4ATtMCgYAL4Ji+0yJTisafJPH7AET1ttoNxHRak11TQ6Za h003hWOSbJkGZe0ka37mVk0cN8iW/3WshoctMAXMy8Z587dzSR4jZISbX7+AbEzL		uj 🔻 Umieść	w bibliotece 👻 🛛 L
<pre>//DL2dSt/alxuUodpudnRm/PR5qYHy9qFK/GtT/2P22nXePMEEFRTqjMxwUBwXoxd 7w33FQKBgGix46T2iICNLz2+x18J7ul7UBhCuLwvmiKqCNhv8jgsPuTDD/iSngYQ MyNc+yM8ClGZ/YuZortRR/9MfkCBerdj1HmHTbi88SgyefktbpaftLhG3AlX0jXp 7gq7uBq+xfqJuws1pw/praxy/pu8pibeuszpp1zyzFAVtZ0gRq</pre>		bione	Nazwa
END RSA PRIVATE KEY	>	statnie miejsca	klucz.ppk

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

🛃 PuTTY Key Generator 🗾	
File Key Conversions Help	
Key	
No key.	
ż.	
Actions	
Generate a public/private key pair Generate	putty
Load an existing private key file	
Save the generated key Save public key Save private key	i 🛪 Nowy folder
	j · Nowy rolaer
	▲ Nazwa
SSH-1 (RSA)  SSH-2 RSA  SSH-2 DSA	ione
Number of bits in a generated key: 2048	tatnie miejsca

- 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

PuTTY Key Generato	r		<b>X</b>		
ile Key Conversion	ns Help				
Key 3					
Public key for pasting in	nto Open SSH authorized k	evs file:			
ssh-rsa AAAAB3NzaC1yc2EA TtDF76+tmlKtc3JibsSI +HRXbH/5b2LTS9Rs +WolOInZwfFrxZr2IK9	AAADAQABAAABAQCmVtv LUDTuzdo/6ecZF0b4QyDz mIMIs c4Tp1p/61oWr7dX9jWxsQ	rtzvDfJJoRUBKIL8KASz6d2rNjel p8P6J4R+BfXqh/IIYJpa rZBKQMTJOlktXdISS1UCEPumL	r/7s ≜ zd ▼		
Key fingerprint:	ssh-rsa 2048 f7:cd:e0:86:d6:39:3f:c3:c2:40:34:1d:db:5d:97:21				
Key comment:	imported-openssh-key				
Key passphrase:	•••••				
Confirm passphrase:	•••••				
Actions					
Generate a public/priv	ate key pair	Genera	ite		
Load an existing private	e key file	Load			
Save the generated ke	y S	ave public key	te key		
Parameters					
Type of key to generat SSH-1 (RSA)	e: SSH-2 RSA	SSH-2 DSA			
N 1 (1 × 1		00.40	_		

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.

 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.

Category: Session Window Window Bela Connection type: Selection Colours Connection Behaviour Selection Pot 10.0.30 Connection type: Connection Saved Sessions Save	🕵 PuTTY Configuration		-
Session       Basic options for your PuTTY session         Terminal       Specify the destination you want to connect to         Host Name (or IP address)       Port         10.0.0.30       22         Connection type:       Raw         Behaviour       Translation         Selection       Saved Sessions         Colours       Default Settings         Data       Default Settings         Proxy       Save	Category:		
Image: Specify the destination you want to connect to         Image: Window         Image:		Basic options for your PuTTY se	ession
Connection type: Features Connection type: Raw ○ Telnet ○ Rlogin ◎ SSH ○ Serial Load, save or delete a stored session Saved Sessions Selection Colours Colours Connection Default Settings Load Save	⊡ Terminal Keyboard	Specify the destination you want to conne Host Name (or IP address) 10.0.0.30	Port 22
Appearance     Appearance     Appearance     Appearance     Load, save or delete a stored session     Saved Sessions     Selection     Selection     Default Settings     Load     Save     Save	- Features ⊡ Window	Connection type: Raw C Telnet Rlogin O SS	H 🔘 Serial
Selection     Selection     Colours     Default Settings     Load     Save     Save	···· Appearance ···· Behaviour ···· Translation	Load, save or delete a stored session Saved Sessions	_
Connection Save	Selection Colours	ssh Default Settings	Load
T TOXY	Connection Data Para	ssh	Save
··· Telnet Delete	Telnet Rlogin		Delete

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

ᄰ ubuntu@dlp: ~		
login as: ubuntu		
Authenticating with public key "imp	ported-openssh-key"	
Passphrase for key "imported-openss	sh-key":	
Welcome to Ubuntu 18.04.1 LTS (GNU,	Linux 4.15.0-29-generic	x86_64)
* Documentation: https://help.ubu	untu.com	
* Management: https://landscap	pe.canonical.com	
* Support: https://ubuntu.c	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 22:38:22 201 ubuntu@dlp:~\$	18 from 10.0.0.51	

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

ocour o								
ubuntu@dlp:	~\$	pwd						
/home/ubunt	u							
ubuntu@dlp:	~\$	1s -la	1					
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	1	root	root	271	Oct	1	21:00	.bash_history
-rw-rr	1	ubuntu	ubuntu	220	Aug	28	14:33	.bash_logout
-rw-rr	1	ubuntu	ubuntu	3771	Aug	28	14:33	.bashrc
drwx	2	ubuntu	ubuntu	4096	Aug	28	14:35	
drwx	3	ubuntu	ubuntu	4096	Aug	28	14:35	
drwxrwxr-x	3	ubuntu	ubuntu	4096	Oct	1	22:39	
-rw-rr	1	root	root	10	Oct	1	21:38	.nanorc
-rw-rr	1	ubuntu	ubuntu	807	Aug	28	14:33	.profile
drwx	2	ubuntu	ubuntu	4096	Oct	1	22:41	
-rw-rr	1	ubuntu	ubuntu	0	Aug	28	14:36	.sudo_as_admin_successful
-rw	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.

sshuser@10.0.0.30 bh	SFTP -	
3	Nazwa <u>h</u> osta	Numer po <u>r</u> tu
	10.0.0.30	22 🚔
	Nazwa <u>u</u> żytkownika Hasł <u>o</u>	
	Zapisz 🔽 Anuluj	Zaawansowane 🖛

b) Podłącz plik klucza prywatnego.

Zaawansowane ustawienia	a połączenia	? X			
Środowisko Katalogi Kosz SFTP Powłoka Połączenie Proxy Tunel SST Uwierzytelnienie Błędy Uwaga	<ul> <li>Pomiń całkowicie identyfikacje (SSH-2)</li> <li>Opcje uwierzytelnienia</li> <li>Spróbuj uwierzytelniania używając Pagenta</li> <li>Spróbuj uwierzytelnienia z 'interakcją-z-kławiatury' (SSH2)</li> <li>Odpowiadaj hasłem na pierwszy znak zachęty</li> <li>Spróbuj uwierzytelniania TIS lub CryptoCard (SSH1)</li> </ul>				
	Parametry identyfikacyjne Pozwól na interakcję z lokalnym agentem kluczy (agent-fw) Plik klucza prywatnego C: Wsers \admin\Desktop \klucz.ppk				
	GSSAPI				
Kolor 🔻	OK Anuluj	Pomoc			

c) Zapisz sesję jak poniżej.



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

🔁 Logowanie 🔻

- 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.