Ćwiczenie 3

SSH – Linux serwer

# Definicje

**SSH** (ang. secure shell) to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer a od wersji 2 nawet w architekturze serwer klient.

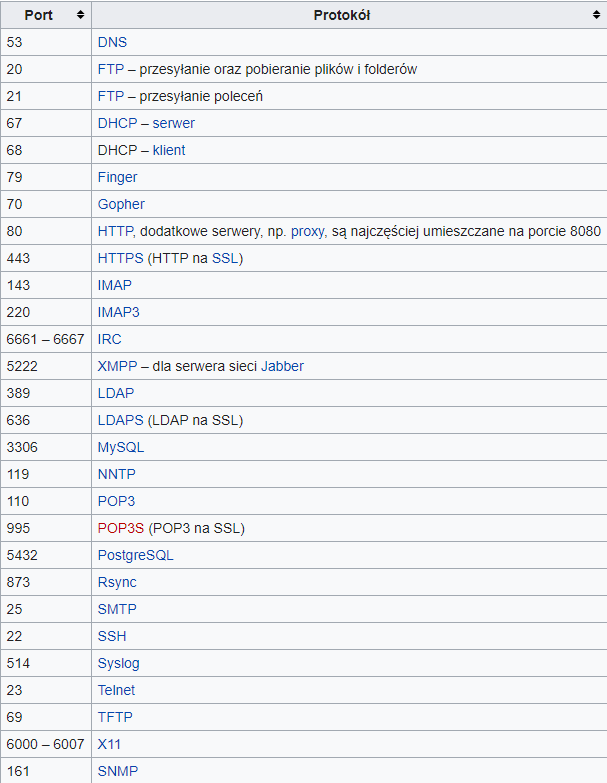
W ścisłym znaczeniu SSH to tylko następca protokołu Telnet, służącego do terminalowego łączenia się ze zdalnymi komputerami. SSH różni się od Telnetu tym, że transfer wszelkich danych jest zaszyfrowany oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów. W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań. Wspólną cechą wszystkich tych protokołów jest identyczna z SSH technika szyfrowania danych i rozpoznawania użytkownika. Obecnie protokoły z rodziny SSH praktycznie wyparły wszystkie inne mniej bezpieczne protokoły, takie, jak np. rlogin czy RSH.

**Secure copy lub SCP –** bezpieczny transfer plików pomiędzy lokalnym a zdalnym lub między zdalnymi komputerami, używając protokołu Secure Shell (SSH). Skrót SCP odnosi się do dwóch powiązanych ze sobą rzeczy: protokołu SSH oraz polecenia cp.

**SFTP** (ang. SSH File Transfer Protocol) – protokół komunikacyjny typu klient-serwer, który umożliwia przesyłanie plików poprzez sieć TCP/IP.

Przesyłając plik przy użyciu protokołu FTP uzyskujemy dobre przepływności, ale nie zyskujemy bezpieczeństwa – nasze hasła i dane nie są szyfrowane podczas przysyłania, co potencjalnie stwarza zagrożenie ich kradzieży. Znaczną poprawę bezpieczeństwa przynosi protokół SFTP, który nie wymaga obecności serwera FTP, a przesyłane dane są szyfrowane z wykorzystaniem klucza szyfrującego.

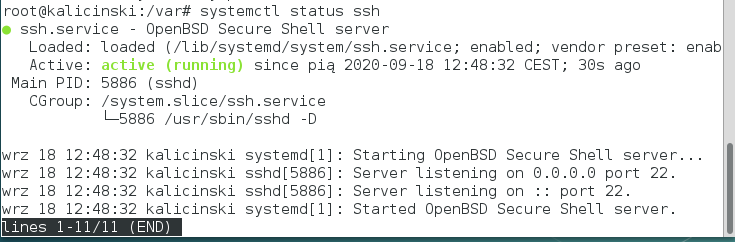
**SFTP nie powinien być mylony z protokołem FTPS, który jest rozszerzeniem protokołu FTP.**



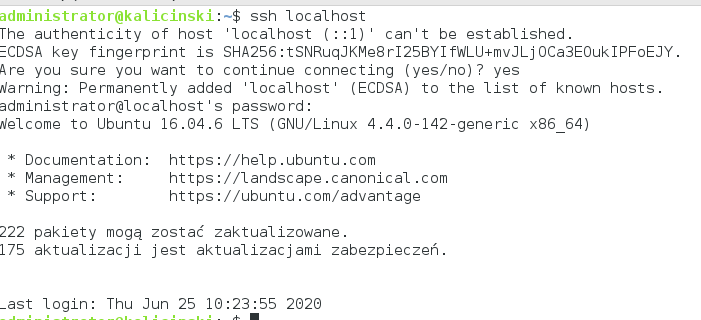
# Instalacja serwera SSH



Rysunek - Instalacja pakietu na serwerze



Rysunek - Sprawdzenie działania usługi



Rysunek - Sprawdzenie logowania się lokalnie (użytkownik nie będący rootem)



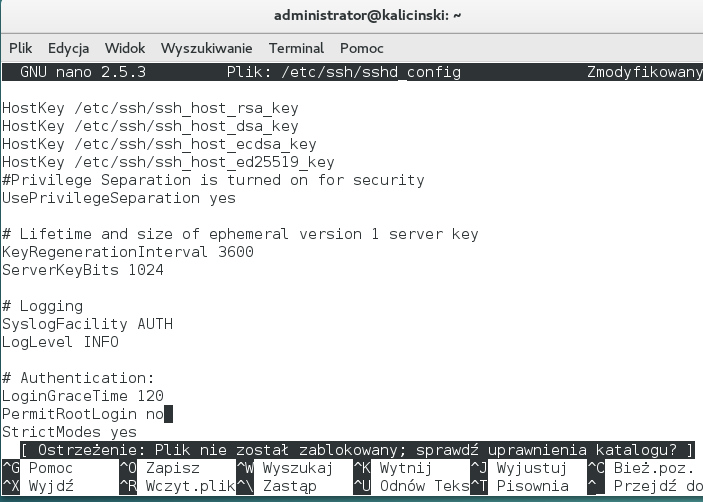
Rysunek - Aby wylogować się używamy kombinacji klawiszowej Ctrl+D



Rysunek - Instalacja pakietu na kliencie

# 

# Konfiguracja serwera SSH

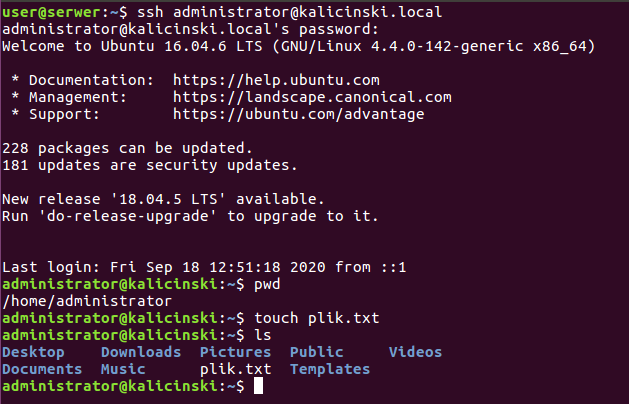


Rysunek - Sprawdzamy czy root może się logować (nano /etc/ssh/sshd\_config)



Rysunek - Reset usługi

# Test na kliencie



Rysunek - Sprawdzamy logowanie zdalne z klienta (zalogowano zdalnie na serwerze). Możemy z tego miejsca utworzyć plik na serwerze.

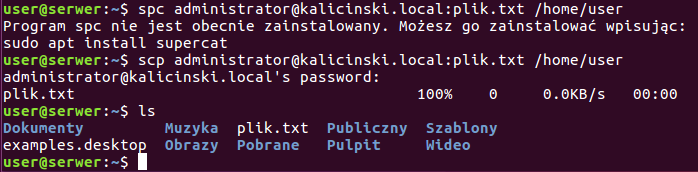


Rysunek - Pojawił się na Ubuntu Server

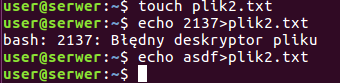


Rysunek - Ctrl+D” kończy połączenie

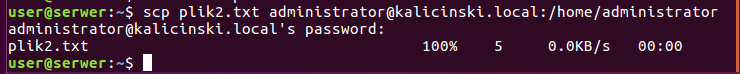
# Kopiowanie za pomocą SCP



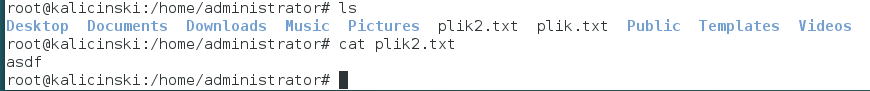
Rysunek - Kopiujemy plik z serwera na klienta



Rysunek - Tworzymy plik tym razem na serwerze

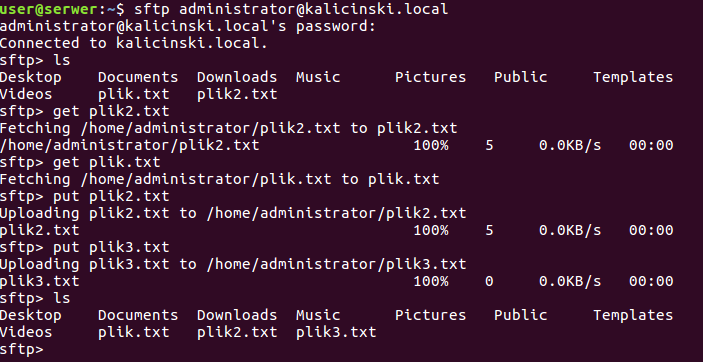


Rysunek - I przesyłamy w drugą stronę



Rysunek - Jak widać na Ubuntu Server przesłało się

# Kopiowanie za pomocą SFTP



Rysunek - Używając polecenie „sftp” łączymy się z serwerem. Pobraliśmy 2 pliki (plik.txt, plik2.txt), a wysłaliśmy plik2.txt oraz plik3.txt

Składnia polecenia:

sftp (nazwa\_użytkownika\_zdalnego)@(nazwa\_hosta\_zdalnego)

Polecenie do zarządzania plikami i katalogami np. „ls”, „pwd”, „mkdir” itd. działają normalnie

Polecenie „get” pobiera plik

Polecenie „put” wysyła plik

Spis treści

[Definicje 1](#_Toc53154930)

[Instalacja serwera SSH 2](#_Toc53154931)

[Konfiguracja serwera SSH 3](#_Toc53154932)

[Test na kliencie 4](#_Toc53154933)

[Kopiowanie za pomocą SCP 5](#_Toc53154934)

[Kopiowanie za pomocą SFTP 6](#_Toc53154935)