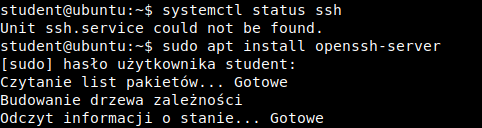
**Jakub Dudek**

**Sprawozdanie SSH**

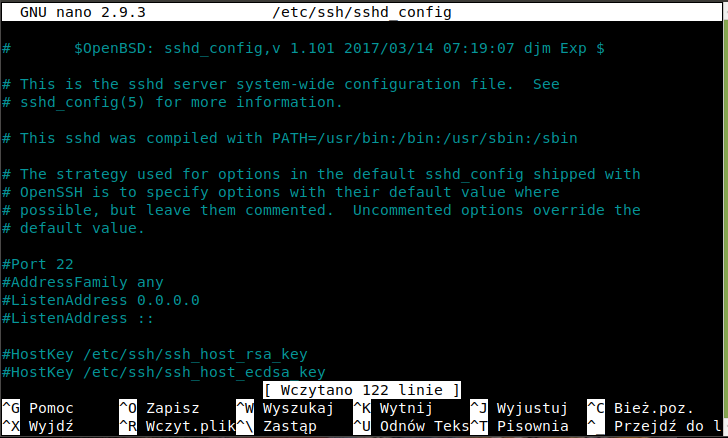
**1. Opisz do czego służy z protokół SSH. Jeżeli serwer ssh nie jest zainstalowany na maszynie wirtualnej zainstaluj go - opisz kroki niezbędne w celu instalacji, podaj nazwę i lokalizację pliku zawierającego konfigurację  
serwera SSH (podaj fragment jego zawartości)**

SSH jest zwykle używany do zdalnego logowania z komputerem i wykonywania poleceń, ale obsługuje także tunele, przekazywanie portów TCP i X11. Możliwe jest przesyłanie plików przy użyciu protokołów przesyłania plików SSH (SFTP) lub SCP. SSH używa modelu klient-serwer. SSH jest ważny dla przetwarzania danych w chmurze, aby rozwiązać problemy z łącznością, unikając problemów bezpieczeństwa związanych z eksponowaniem wirtualnej maszyny w chmurze. Tunel SSH może zapewnić bezpieczną ścieżkę przez Internet, poprzez zaporę ogniową do maszyny wirtualnej.

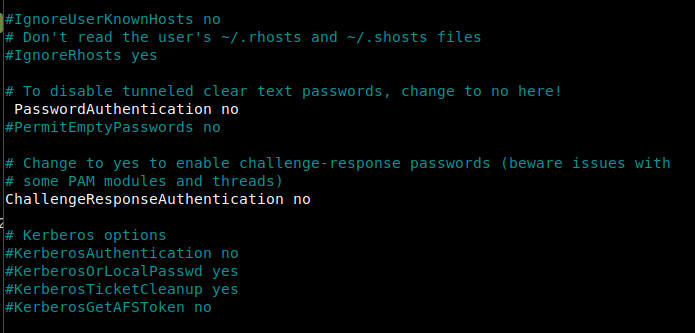


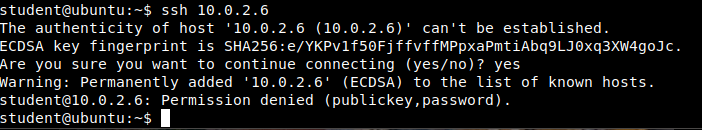
Aby zainstalować ssh należy użyć polecenia apt install openssh-server.

Plik konfiguracyjny nazywa się sshd\_config i znajduje się w /etc/ssh/.



**2. Opisz i przetestuj opcję Disable Password Authentication**

****

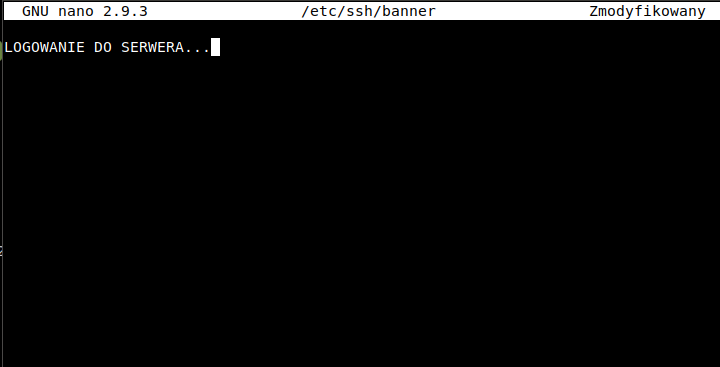
****

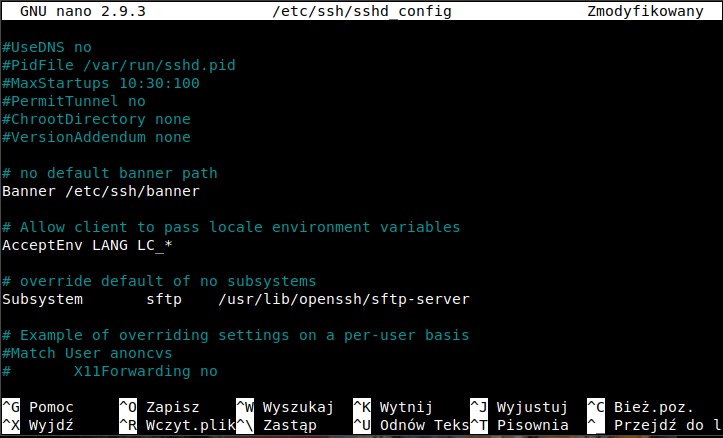
Disable Password Authentication wyłacza możliwość zalogowania używając hasła. Możemy zalogować się za pomocą klucza.

**3. Utwórz wiadomość (banner) pojawiający się w momencie logowania do  
serwera)**

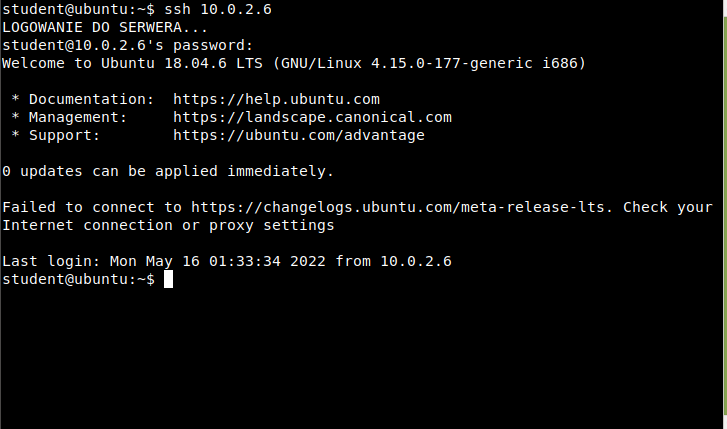
****

Trzeba utworzyć plik w którym umieścimy nasz baner. Następnie edytujemy plik sshd\_config i podajemy ścieżkę do naszego banera. Na końcu restartujemy sshd service.



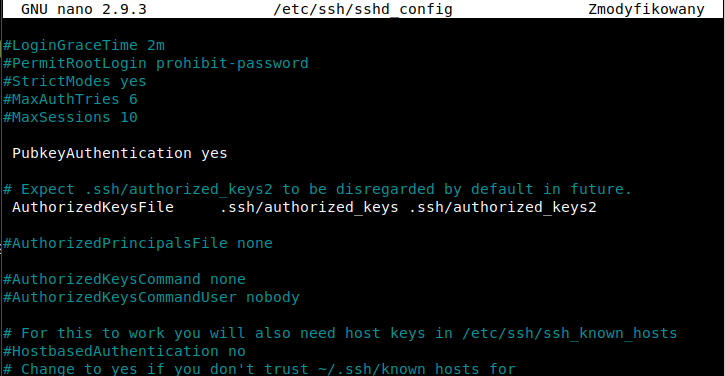
****

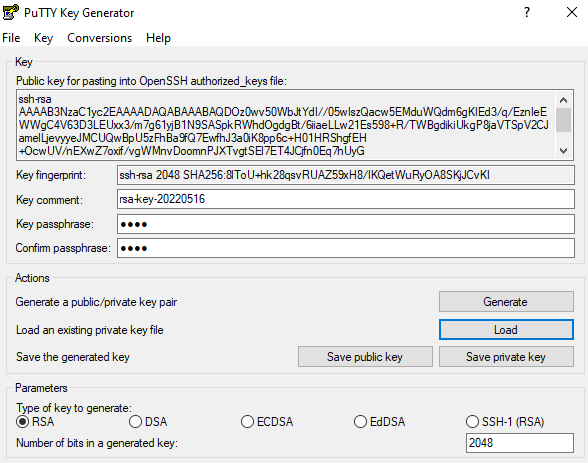
****

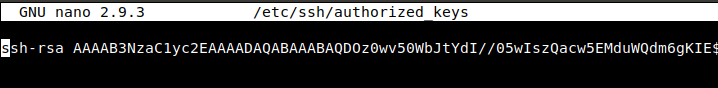
****

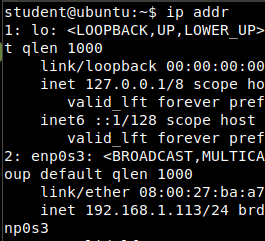
**4. Opisz dostępne opcje związane z kryptografią klucza publicznego i  
prywatnego. Zaimplementuj na serwerze rozwiązanie z nim związane.  
a. Na maszynie klienta (Windows) zainstaluj klienta (putty), na maszynie  
klienta wygeneruj klucze dla użytkownika student (puttygen)  
umieścić klucz publiczny na serwerze zrestartuj serwer SSH, sprawdź  
możliwość zalogowania się na serwerze.**

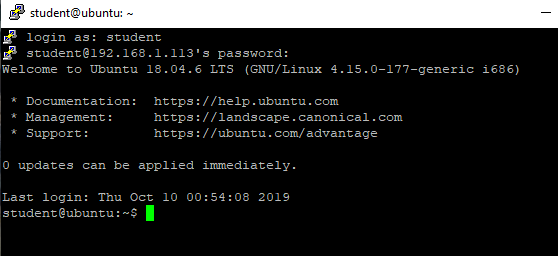
Musimy włączyć możliwość zalogowania poprzez klucz publiczny w pliku sshd\_config oraz stworzyć plik authorized\_keys i umieścić w nim nasz wygenerowany klucz.



****

****

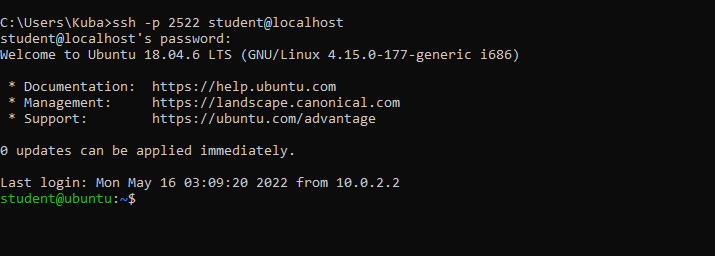
****

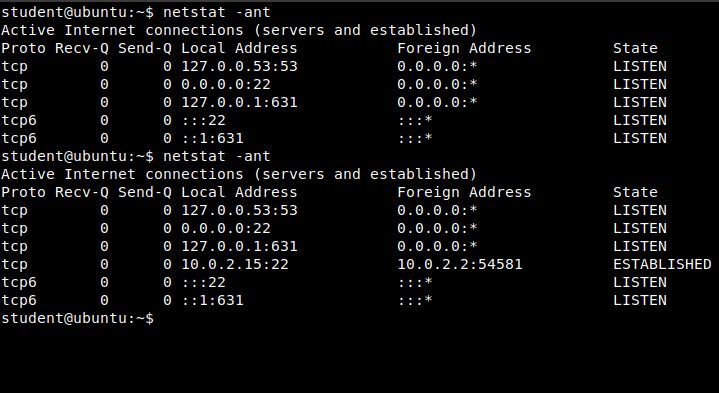
****

**5. Opisz opcję „forwarding” wraz z przykładem jej zastosowania.  
Zademonstruj użycie tunelowania. (programem nestat wykaż otwarte porty  
na maszynie kliencie). Omów różnice i przykłady zastosowań dla\*  
i. local port forwarding  
ii. remote port forwarding  
iii. dynamic port forwarding**

Forwarding jest działaniem, mającym na celu udostępnienie danej zawartości z sieci lokalnej komputerom nienależącym do tej sieci przez wykorzystanie określonego portu. Jest to standardowa funkcja, którą oferuje praktycznie każdy router.







Local Port Forwarding. - Lokalne przekazywanie portu jest najczęściej używaną formą przekierowania, która zapewnia **bezpieczne przesyłanie danych z aplikacji klienckiej uruchomionej na komputerze.** Pozwala użytkownikowi połączyć się z innym serwerem za pośrednictwem **bezpiecznego tunelu** i przesłać informacje i dane do określonego miejsca docelowego lub portu. Zapory sieciowe, które blokują określone strony, mogą być również pomijane podczas korzystania z lokalnego przekazywania portu.

Remote Port Forwarding. - Ten typ przekierowania portu pozwala każdemu na zdalnym serwerze połączyć się z portem TCP. Zdalne przekierowanie portu jest przydatne **przy ustalaniu zewnętrznego dostępu do wewnętrznego serwera internetowego**, najczęściej używanego przez pracowników zdalnych podczas uzyskiwania dostępu do bezpiecznego serwera z domu.

Dynamic Port Forwarding. - Jest to rzadkie przekierowanie z portu, które pozwala na przebicie się przez zaporę sieciową za pomocą tak zwanych zapór firewall. **Umożliwia klientom ustanowienie bezpiecznego połączenia za pośrednictwem zaufanego serwera**, który działa jako pośrednik, przesyłając dane do innych serwerów. Może służyć do zapewnienia dodatkowego bezpieczeństwa dla użytkownika podłączonego do niezaufanej sieci, na przykład w kawiarni lub hotelu.