

Laboratorium 1 – Konfiguracja środowiska serwera

1 INFORMACJE WSTĘPNE

1.1 LOGOWANIE DO SERWERA

Dla potrzeb zajęć laboratoryjnych skonfigurowany został serwer oparty o środowisko systemowe Linux Centos 8. Dostęp zdalny do tego serwera jest możliwy pod numerem IP **212.182.61.57**. Logowanie jest możliwe przy pomocy kont przygotowanych dla każdego studenta. Identyfikatory są w postaci **studentNN** (gdzie $N \in [0-9]$) a hasło inicjalnie jest: **#@\$to4482** Przyporządkowanie identyfikatorów do studentów prezentuje poniższa tabela.

Numer albumu	Identyfikator	Hasło początkowe
13951	student01	#@\$to4482
14558	student02	#@\$to4482
13944	student03	#@\$to4482
13933	student04	#@\$to4482
13979	student05	#@\$to4482
13963	student06	#@\$to4482
13926	student07	#@\$to4482
13965	student08	#@\$to4482
13940	student09	#@\$to4482
13955	student10	#@\$to4482
14448	student11	#@\$to4482

Podstawową formą zdalnego dostępu do serwera jest dostęp poprzez protokół SSH pozwalający na dostęp do konta „shellowego” i przesyłania plików poprzez SCP. Przykładowe programy pozwalające na dostęp: putty, winscp, VS Code.

Jeżeli w opisie występuje odniesienie do nazwy użytkownika w formie studentNN to oczywiście należy je zamienić specyficznym dla danego studenta identyfikatorem. Folder domowy użytkownika studentNN jest /home/studentNN, natomiast folder w którym konfigurowany będzie wirtualny host WWW jest /var/www/studentNN.

2 ZADANIA DO WYKONANIA

2.1 ZABEZPIECZENIE ZDALNEGO DOSTĘPU

2.1.1 Dostęp zdalny z systemu WIN10 przy pomocy wbudowanego klienta OpenSSH

System Win10 posiada wbudowanego klienta protokołu SSH pozwalającego na zdalny dostęp. Klient ten – OpenSSH – jest domyślnie wyłączony w systemie. Aby go używać należy go włączyć przy pomocy funkcji zarządzania dodatkowymi komponentami systemu operacyjnego.

Proszę włączyć na swoim komputerze klienta SSH w oparciu o [dostępny tu opis](#). Proszę zwrócić uwagę aby włączyć tylko komponent „OpenSSH Klient” i pozostawić komponent „OpenSSH Serwer” wyłączony.

Po włączeniu OpenSSH w systemie Win10 polecenie **ssh** będące klientem SSH będzie dostępne do użycia w konsoli systemowej. Z serwerem wykorzystywanym na zajęciach można się połączyć przy pomocy polecenia:

```
ssh studentNN@212.182.61.57
```

2.1.2 Zmiana hasła

Początkowo wszyscy studenci mają takie samo hasło pozwalające na dostęp do systemu. Ze względów bezpieczeństwa należy je zmienić na jakieś inne. W tym celu należy zalogować się do serwera poprzez **ssh** i przy użyciu polecenia **passwd studentNN** zmienić hasło na nowe. Procedura zmiany hasła będzie wymagała podania starego i dwukrotnego podania nowego hasła.

2.1.3 Konfiguracja podpisu cyfrowego do uwierzytelniania dla SSH

2.1.3.1 Konfiguracja SSH na PC (WIN10)

Protokół SSH będzie stosowany do dostępu do serwera w celu ułatwienia dostępu należy skonfigurować uwierzytelnianie bazujące na podpisie cyfrowym. Dzięki temu nie będzie konieczności podawania hasła przy połączeniach programem **ssh**.

Najpierw należy na swoim komputerze z WIN10 wygenerować klucz prywatny i publiczny stosowany do uwierzytelniania. W tym celu należy otworzyć konsolę tekstową w systemie WIN10 i użyć polecenia:

```
ssh-keygen
```

które jest elementem składowym pakietu OpenSSH. Polecenie to w katalogu **.ssh** w katalogu domowym użytkownika (proszę zwrócić uwagę gdzie dokładnie) utworzy dwa pliki **id_rsa** i **id_rsa.pub**. Plik **id_rsa** jest kluczem prywatnym a **id_rsa.pub** kluczem publicznym.

2.1.3.2 Konfiguracja SSH na serwerze (Linux)

Po zalogowaniu przez SSH do serwera należy użyć tego samego polecenia **ssh-keygen** do wygenerowania kluczy szyfrujących używanych do uwierzytelniania na serwerze.

W kolejnym kroku należy utworzyć plik **/home/studentNN/.ssh/authorized_keys** zawierający klucz publiczny wygenerowany uprzednio na systemie WIN10 (plik **id_rsa.pub**).

W tym celu proszę skopiować plik **id_rsa.pub** na serwer. Można to wykonać poprzez następujące polecenie wydane w konsoli tekstowej (WIN10) z katalogu gdzie znajdują się generowane poprzednio (pkt. 2.1.3.1) klucze szyfrujące.

```
scp id_rsa.pub studentNN@212.182.61.57:/home/studentNN
```

i dopisać go do pliku **/home/studentNN/.ssh/authorized_keys** wydając następujące polecenie na serwerze.

```
cat /home/studentNN/id_rsa.pub >> /home/studentNN/.ssh/authorized_keys
```

Należy jeszcze zmienić na serwerze uprawnienia do pliku `authorized_keys` tak by tylko właściciel miał uprawnienia do zapisu, pozostali tylko do odczytu:

```
chmod 644 /home/studentNN/.ssh/authorized_keys
```

Oraz do folderu `/home/studentNN/.ssh` :

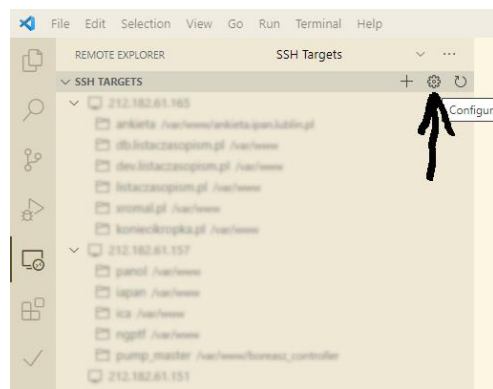
```
chmod 700 /home/studentNN/.ssh
```

Po przeprowadzonej poprawnie konfiguracji uwierzytelniania kryptograficznego w celu połączenia z serwerem po wydaniu polecenia `ssh studentNN@212.182.61.57` nie będzie konieczności podawania hasła.

2.1.4 Konfiguracja zdalnego dostępu w edytorze VS Code

Do pracy zdalnej będzie wykorzystywany edytor VS Code. Pozwala on na wygodną edycję bezpośrednio na serwerze plików dostępnych poprzez protokół SSH. Proszę zainstalować edytor VS Code (<https://code.visualstudio.com/>) i upewnić się że są w nim zainstalowane dodatki: „Remote – SSH” i „Remote - SSH: Editing Configuration”. Jeżeli te dodatki nie są zainstalowane proszę je zainstalować.

Na tym etapie w VSCode dostępne powinno być widoczne poniżej menu/grupa narzędzi o nazwie „Remote explorer”.



Narzędzie to należy skonfigurować używając menu zaznaczonego strzałką na powyższym rysunku. Po jego kliknięciu należy wybrać jedną z oferowanych lokalizacji pliku konfiguracyjnego (najlepiej wybrać plik konfiguracyjny w katalogu domowym użytkownika) po czym w edytorze otworzony zostanie plik konfiguracyjny.

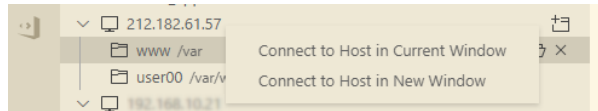
Proszę do tego pliku dodać następującą zawartość (wcięcia w drugim i trzecim wierszu mają znaczenie):


```
Host 212.182.61.57
```

```
User studentNN
```

```
HostName 212.182.61.57
```

Po zapisaniu konfiguracji wpis dotyczący hosta 212.182.61.57 powinien się pojawić w narzędziu „Remote explorer”. I będzie można połączyć się z tym hostem w VSCode. Opcje stosowane do połączenia SSH są dostępne w menu kontekstowym otwartym na numerze ip hosta 212.182.61.57 (patrz obrazek poniżej).



Po połączeniu s serwerem ikona  pozwala na otwarcie konkretnego katalogu na zdalnym hoście. W zakładce „Explorer” wtedy są dostępne pliki i foldery zawarte w otwartym katalogu.

Po połączeniu ze zdalnym hostem również edytorze VSCode możemy otworzyć zdalną konsolę wiersza poleceń. Jeżeli nie pojawi się automatycznie w dolnej części okna edytora należy ją otworzyć przy pomocy menu Terminal->New Terminal.

2.2 KONFIGURACJA ŚRODOWISKA BAZODANOWEGO

2.2.1 Utworzenie bazy danych

W praktyce każdy serwis WWW wymaga do funkcjonowania bazy danych. W środowisku serwerowym przygotowanym na laboratoria serwerem bazodanowym jest oprogramowanie MySQL/MariaDBmysql 8.0.

Dla potrzeb pierwszego środowiska wykorzystywanego na ćwiczeniach przygotuj bazę danych. W tym celu trzeba zrobić dwie rzeczy: utworzyć bazę danych i utworzyć użytkownika posiadającego dostęp do bazy danych:

- Zaloguj się do serwera przez SSH jako studentNN.
- Połącz się z serwerem bazodanowym przy pomocy programu `mysql`. Zwróć uwagę że połączenie wymagało podania hasła (bezpośrednio po opcji „-p”).

```
mysql -p#@$1o4482
```

- Utwórz nową bazę danych wydając poniższe polecenie w programie `mysql`. Zastosuj swoją nazwę bazy danych zamiast przykładowej `db_name`. Zwróć uwagę że zastosowano jawne określenie sposobu kodowania znaków w bazie danych i ich porównywania:

```
CREATE DATABASE db_name CHARACTER SET utf8 COLLATE utf8_bin;
```

- Utwórz użytkownika stosowanego do dostępu do tej bazy danych (zastąp `db_user` swoją nazwą użytkownika i `password` jakimś hasłem). Zanonuj te informacje:

```
CREATE USER "db_user"@"localhost" IDENTIFIED BY "password";
```

- Nadaj użytkownikowi uprawnienia do bazy danych (zastąp `db_name` nazwą swojej bazy danych, `db_user` swoją nazwą użytkownika i `password` jakimś hasłem). Aby uprawnienia nowego użytkownika na pewno już obowiązywały wydaj polecenie:

```
GRANT ALL ON db_name.* TO "db_user"@"localhost";
```

- Aby nowe uprawnienia na pewno były już widoczne przez serwer MySQL wydaj polecenie:

```
FLUSH PRIVILEGES;
```

- Zanotuj nazwę bazy danych, identyfikator użytkownika i jego hasło do późniejszego wykorzystania.