

Politechnika Częstochowska
Wydział Inżynierii Mechanicznej i Informatyki



Laboratorium z przedmiotu
Bezpieczeństwo komunikacji elektronicznej

Sprawozdanie nr 8

FTP

Damian Łukasik
nr. 112993
II stopień, 2 semestr , 1 rok

Częstochowa 28 grudnia 2015 r.

1. Cel ćwiczenia laboratoryjnego

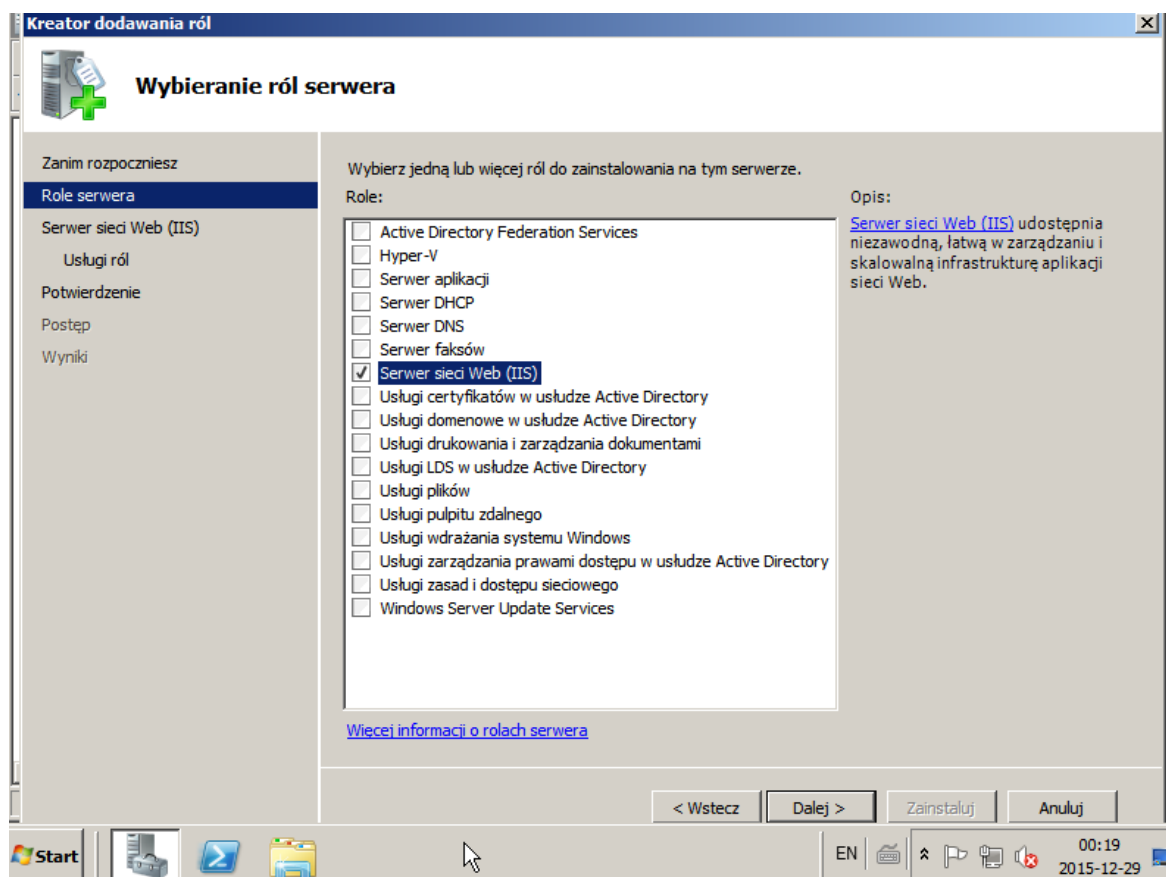
Celem ćwiczenia laboratoryjnego było zapoznanie się z usługą serwera FTP w Windows Server 2008. Z przeprowadzonego ćwiczenia zostały wyciągnięte wnioski. Do sprawozdania załączono zrzuty ekranu w postaci *printscreenów*.

2. Opis ćwiczenia

W trakcie laboratorium przewidziano instalację serwera FTP, konfigurację katalogów i użytkowników oraz nawiązaniu połączenia poprzez program WinSCP.

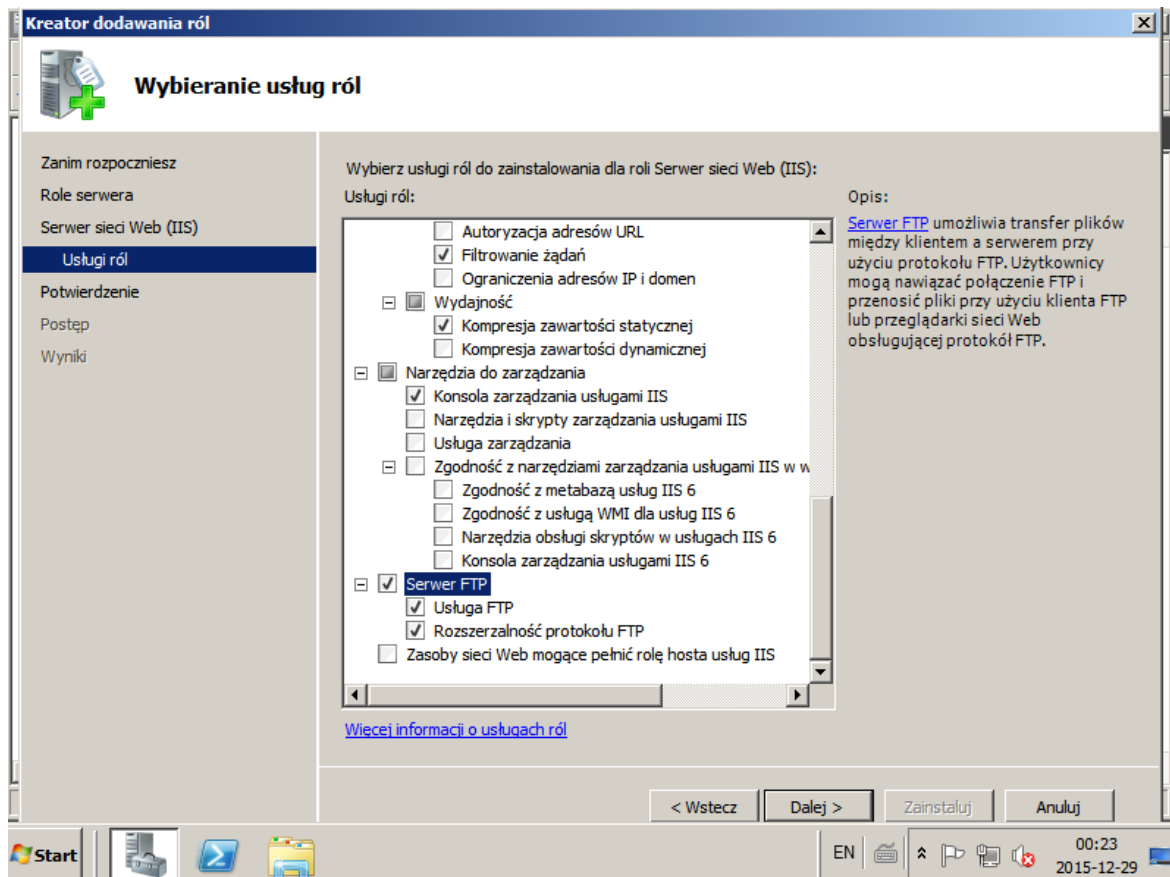
3. Przebieg ćwiczenia laboratoryjnego

W pierwszej kolejności zainstalowano serwer FTP. W tym celu najpierw dodano rolę Web Server (IIS):

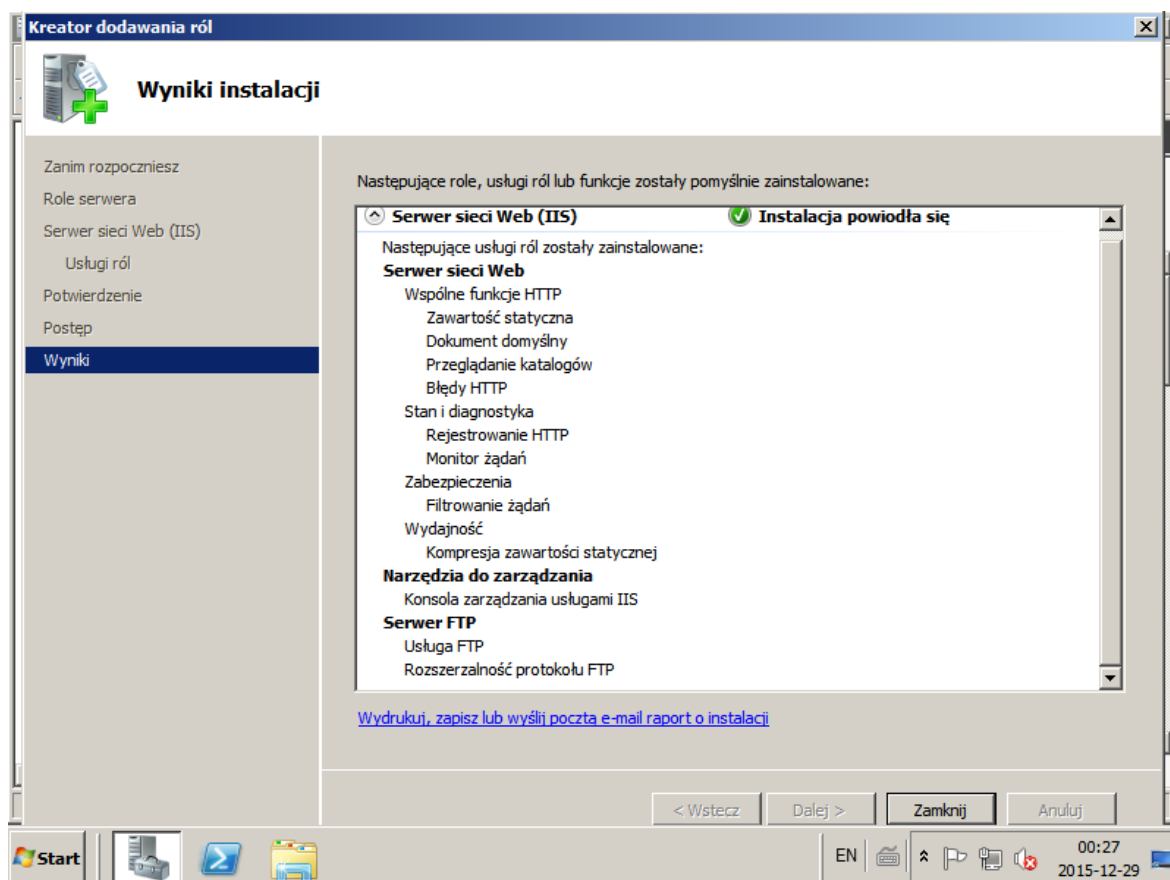


Rys1. Wybranie roli Web Server.

Następnie wybrano komponent serwera IIS - Server FTP (*FTP Service* oraz *FTP Extensibility*). Po poprawnym zainstalowaniu, uruchomiono serwer ponownie.

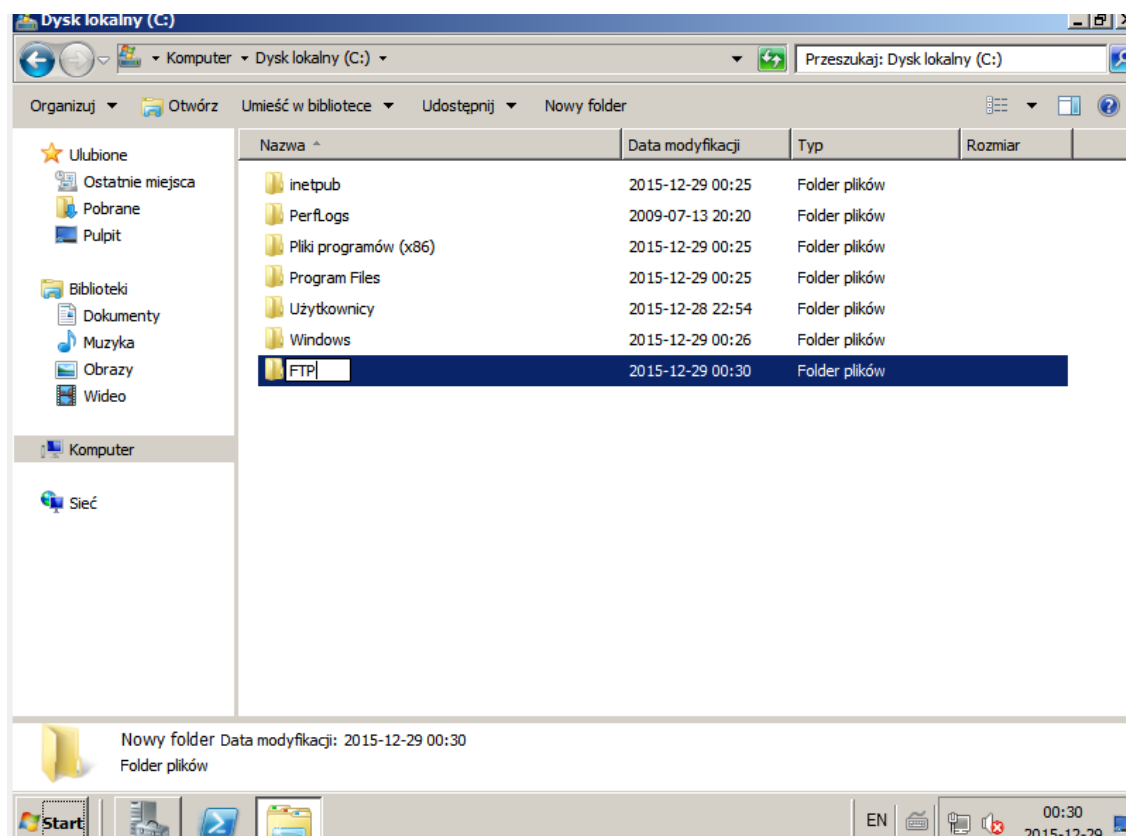


Rys2. Wybranie komponentu Server FTP.



Rys3. Server FTP został zainstalowany pomyślnie.

W drugiej kolejności skonfigurowano katalog i użytkowników. Na początku utworzono katalog, który będzie stanowił korzeń drzewa FTP.



Rys4. Utworzenie katalogu FTP.

Następnie dodano użytkownika FTP w Menedżerze serwera. W tym celu kliknięto prawym przyciskiem myszy na zakładce *Użytkownicy* znajdującej się w rozwiniętej zakładce *Użytkownicy i grupy lokalne* i z listy wybrano *Nowy użytkownik*. Otrzymano okno z dodawaniem nowego użytkownika:

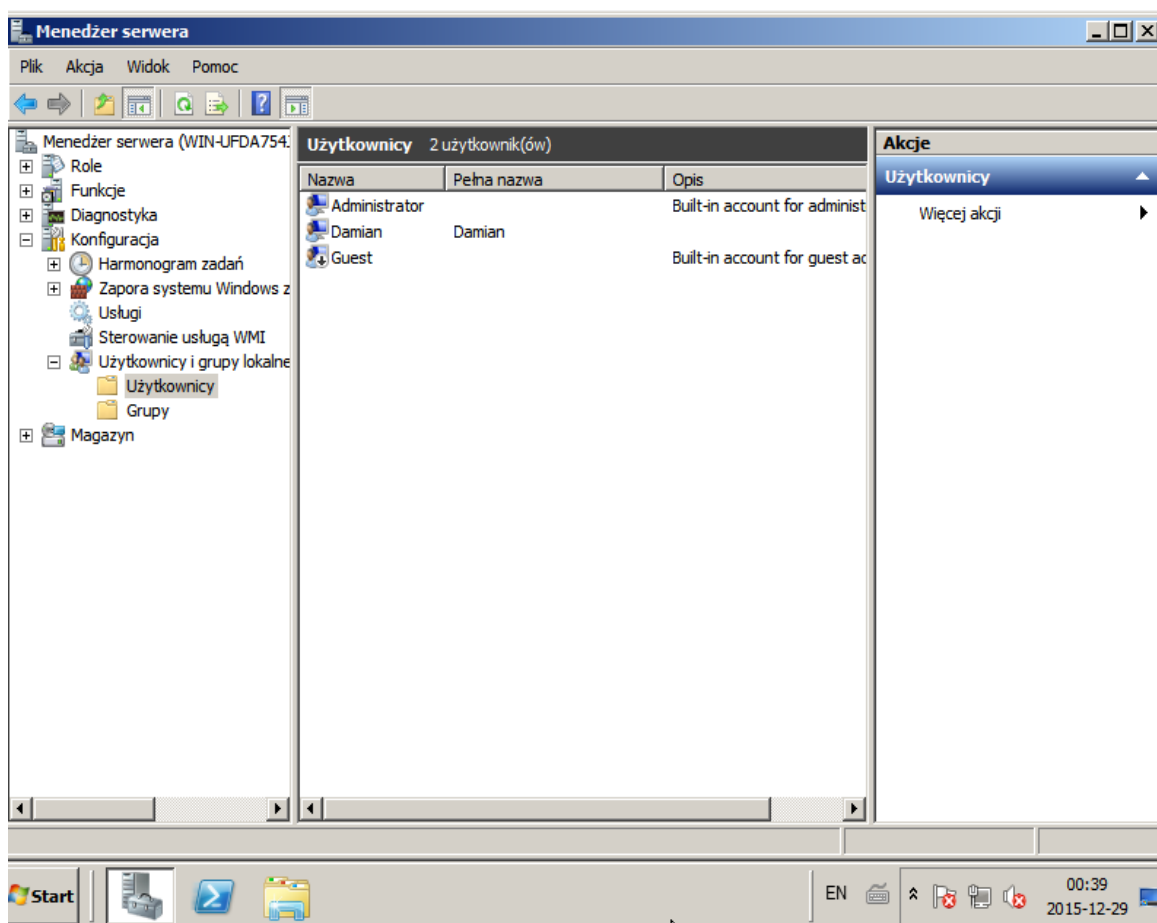
The screenshot shows the 'Nowy użytkownik' dialog box. It contains the following fields and options:

- Nazwa użytkownika:** Damian
- Pełna nazwa:** Damian
- Opis:** (empty text box)
- Hasło:** (password field with 8 dots)
- Potwierdź hasło:** (password field with 8 dots)
- ☒ Użytkownik musi zmienić hasło przy następnym logowaniu
- ☐ Użytkownik nie może zmienić hasła
- ☐ Hasło nigdy nie wygasa
- ☐ Konto jest wyłączone

At the bottom, there are three buttons: 'Pomoc', 'Utwórz', and 'Zamknij'.

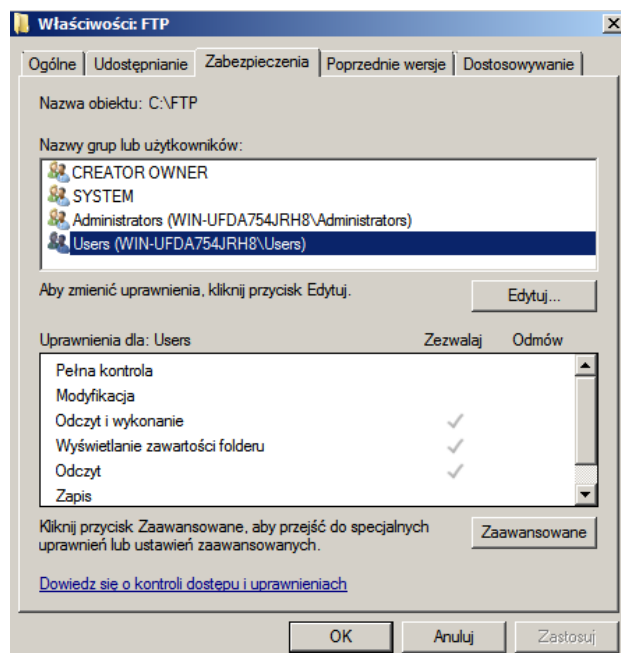
Rys5. Utworzenie nowego użytkownika.

Po wpisaniu nazwy użytkownika i hasła, utworzono nowego użytkownika poprzez naciśnięcie przycisku *Create*.



Rys6. Widok Menadżera serwera z nowoutworzonym użytkownikiem.

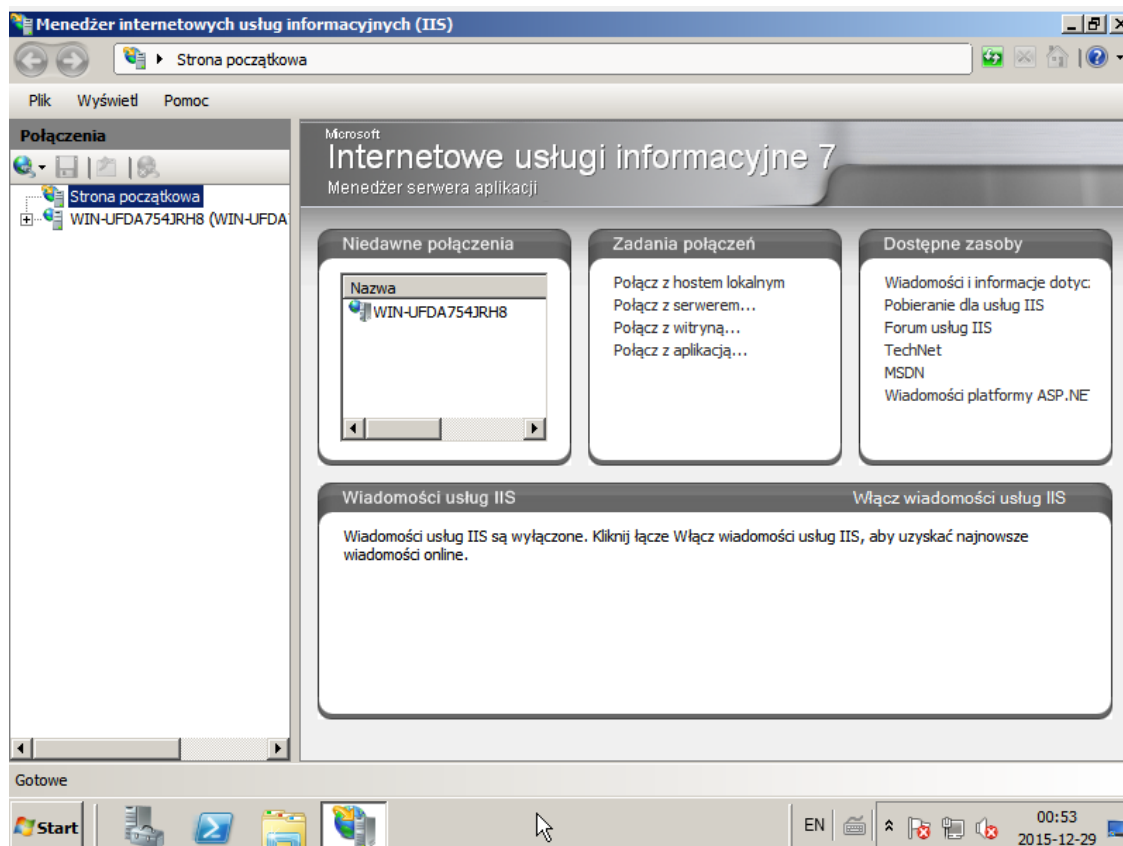
Po utworzeniu katalogu oraz użytkownika, nadano uprawnienia użytkownikowi do korzystania z tego katalogu we właściwościach folderu:



Rys7. Właściwości folderu FTP, zakładka Zabezpieczenia.

Najważniejszymi uprawnieniami są uprawnienia do czytania (*Read*) i wyświetlania listy zawartości folderu (*List folder contents*). Dodatkowo można zaznaczyć również uprawnienia do zapisu (*Write*), dzięki czemu będzie można dodawać nowe pliki do katalogu.

Następnie otworzono Menadżer internetowych usług informacyjnych (IIS):




Rys8. Widok Menadżera internetowych usług informacyjnych (IIS).

Rozwinięto listę, znajdującą się w lewej części okna, a następnie rozwinięto zakładkę *Witryny*. Domyślnie znajduje się tam tylko strona główna IIS. Naciśnięto prawym przyciskiem myszy na zakładkę *Witryny* i wybrano z listy *Dodaj publikację FTP*.

Wybrano z listy adres, który będzie mógł łączyć się z serwerem FTP. Można również wykorzystać wirtualną nazwę dla serwera. Aby użyć bezpiecznego połączenia należy wybrać certyfikat SSL wygenerowany dla serwera na wcześniejszych laboratoriach. Po wprowadzeniu ustawień i kliknięciu *Next* otrzymano okienko z konfiguracją użytkowników FTP.

Dodaj publikację witryny FTP ? X

 **Ustawienia powiązań i protokołu SSL**

Powiązanie

Adres IP: 192.168.0.104 Port: 21

☒ Włącz nazwy hosta wirtualnego:
Host wirtualny (przykład: ftp.contoso.com): ftp.laboratoria.pl

☒ Uruchom automatycznie witrynę FTP

SSL


☐ Brak
☐ Zezwalaj
☒ Wymagaj

Certyfikat SSL: Nie wybrano Wyświetl...

Poprzedni Dalej Zakończ Anuluj

Rys9. Dodawanie publikacji witryny FTP – ustawieni powiązań i protokołu SSL.

Dodaj publikację witryny FTP ? X

 **Informacje dotyczące uwierzytelniania i autoryzacji**

Uwierzytelnienie

☐ Anonimowe
☒ Podstawowe

Autoryzacja

Zezwalaj na dostęp do:
Określeni użytkownicy
Damian

Uprawnienia

☒ Odczyt
☒ Zapis

Poprzedni Dalej Zakończ Anuluj

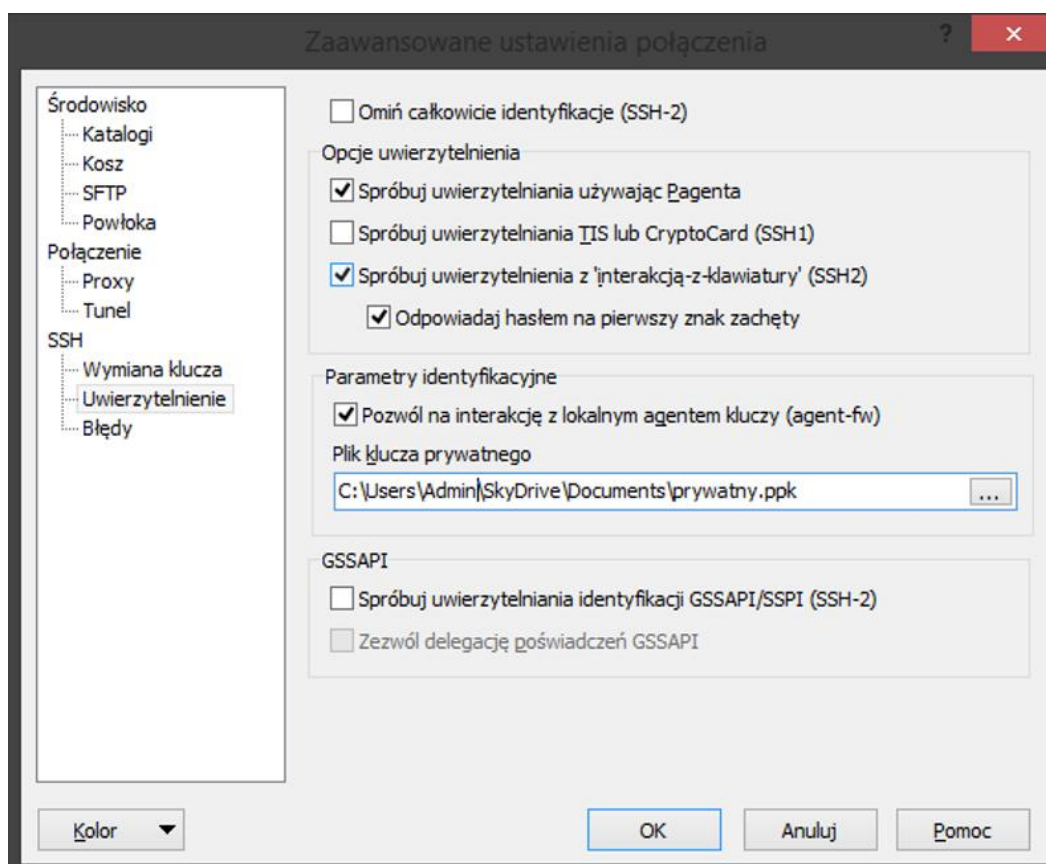
Rys10. Dodawanie publikacji witryny FTP – informacje dotyczące uwierzytelniania i autoryzacji.

Po zakończeniu tej czynności możemy zalogować się do naszego serwera na dwa sposoby:

- Poprzez przeglądarkę.
- Poprzez klienta FTP (np. WinSCP).

W trzeciej kolejności nawiązano połączenie poprzez program WinSCP.

WinSCP – program z rozszerzonymi możliwościami komunikacji z serwerami FTP. Może używać kluczy prywatnych, aby połączyć się z serwerem, na którym znajduje się sparowany klucz publiczny. Do ładowania klucza i jego szybkiego użycia wykorzystuje się program *PuTTY* przeznaczony do szybkiego dodawania klucza prywatnego do połączenia. Aby użyć wcześniej wygenerowanego klucza należy w ustawieniach zaawansowanych w oknie dodawania lub edycji połączenia wybrać zakładkę *SSH > Uwierzytelnienie*, gdzie jest wybierany plik będący kluczem prywatnym dla wpisanego użytkownika.

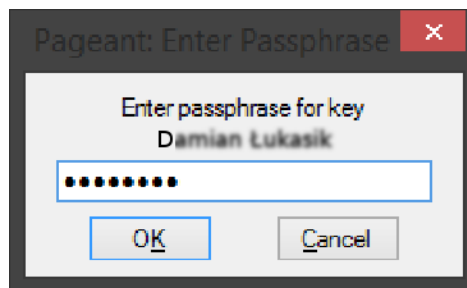


Rys11. Zaawansowane ustawienia połączenia.

W takiej konfiguracji serwer będzie zwracał prośbę o podanie hasła szyfrującego do klucza.

W celu automatycznego dodawania klucza do połączenia razem z naszym hasłem szyfrującym należy po uruchomieniu programu *PuTTY*, w pasku zadań kliknąć prawy przyciskiem myszy opcję *Add Key*.

Po otwarciu klucza zostaniemy poproszeni o jednorazowe podanie hasła:



Rys12. Wprowadzanie hasła.

Od tego momentu przy każdym logowaniu na FTP poprzez program *WinSCP* z wykorzystaniem protokołu SFTP nie ma potrzeby podawania klucza i hasła za każdym razem, dopóki jest uruchomiony program *PuTTY*.

4. Wnioski

Udało się zainstalować, skonfigurować i połączyć z serwerem FTP. Poprzez zastosowanie struktury klucza prywatnego jest możliwe bezpieczne używanie protokołu SFTP do komunikacji z serwerem posiadającym sparowany klucz publiczny. Z kolei program *PuTTY* bardzo upraszcza korzystanie ze struktury klucza prywatnego, ponieważ nie trzeba za każdym razem wpisywać haseł. Przydaje się w sytuacji kiedy serwer ma podniesiony poziom bezpieczeństwa poprzez ograniczenie czasu na odpowiedź użytkownika do kilku sekund. Z tego powodu użytkownik może być zastąpiony przez program, który może wpisać hasło za użytkownika.