Politechnika Częstochowska
Wydział Inżynierii Mechanicznej i Informatyki

Laboratorium z przedmiotu
Bezpieczeństwo komunikacji elektronicznej

Sprawozdanie nr 7

Protokoły uwierzytelniania oparte o certyfikaty

Piotr Zyszcak
nr. 113066
Damian Łukasik
nr. 112993
II stopień, 2 semestr , 1 rok

Częstochowa 28 grudnia 2015 r.

1. Cel ćwiczenia laboratoryjnego

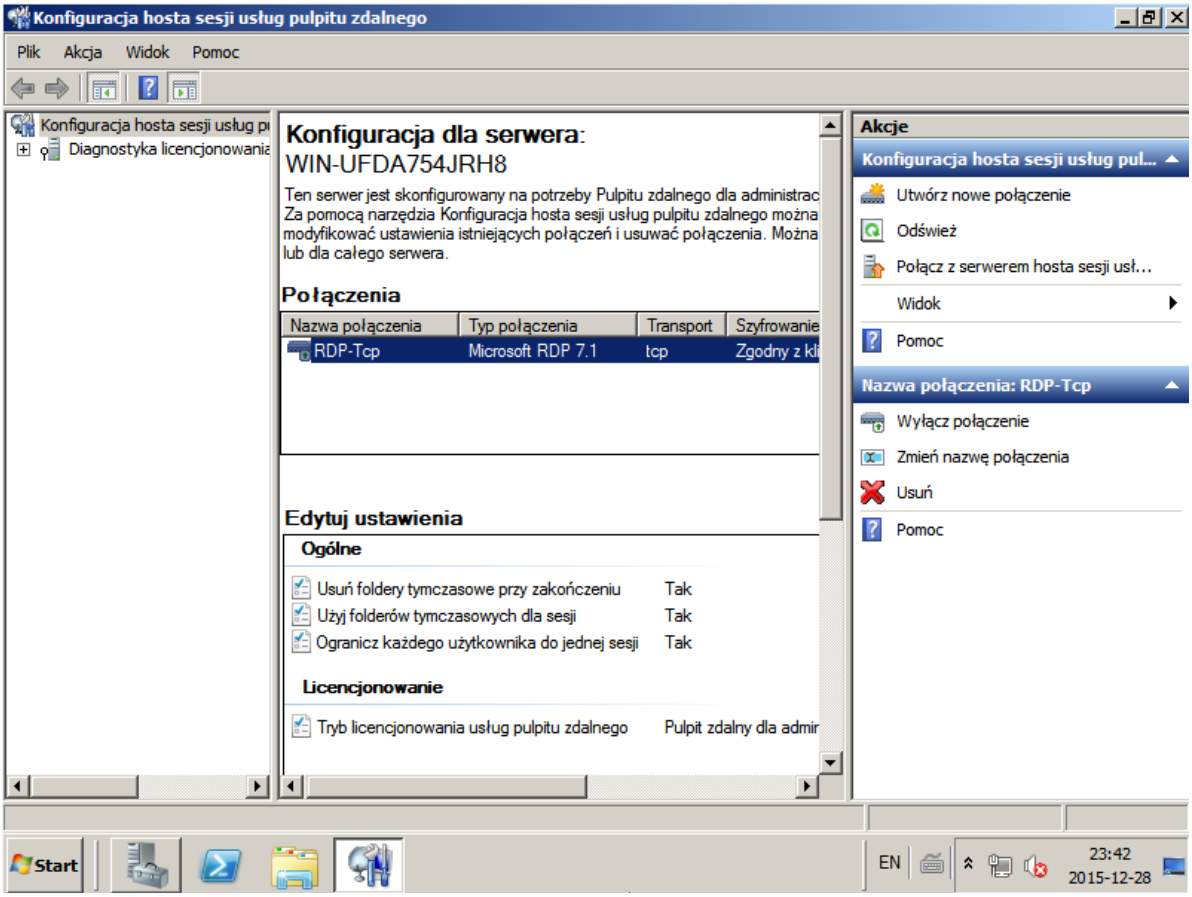
Celem ćwiczenia laboratoryjnego była konfiguracja protokołu TLS/SSL na maszynie z systemem Windows Server 2008. Z przeprowadzonego ćwiczenia zostały wyciągnięte wnioski. Do sprawozdania załączono zrzuty ekranu w postaci *printscreenów*.

2. Opis ćwiczenia

Protokół **TLS** (SSL) - jest to rozwinięcie protokołu SSL (ang. *Secure Socket Layer*) – stworzony przez firmę *NetScape Communications*. TLS gwarantuje nam zachowanie integralności przesyłanych danych. Służy on również do uwierzytelniania serwerów (klientów również). Działa w warstwie prezentacji, gdzie zabezpiecza m.in.: *telnet*, *http*, *POP3* oraz *IMAP*. SSL standaryzuje algorytmy, techniki oraz schematy używane do zapewnienia bezpieczeństwa. Używa on algorytmów szyfrowania symetrycznych oraz asymetrycznych. Do szyfrowania używane są obecnie klucze 128 oraz 40 bitowe. Ważną częścią protokołu SSL są certyfikaty. Posiadają one nazwę domeny i podpisują je zgodnie z Infrastrukturą Klucza Publicznego Urzędu Certyfikacji (*Certificate Authority – CA*).

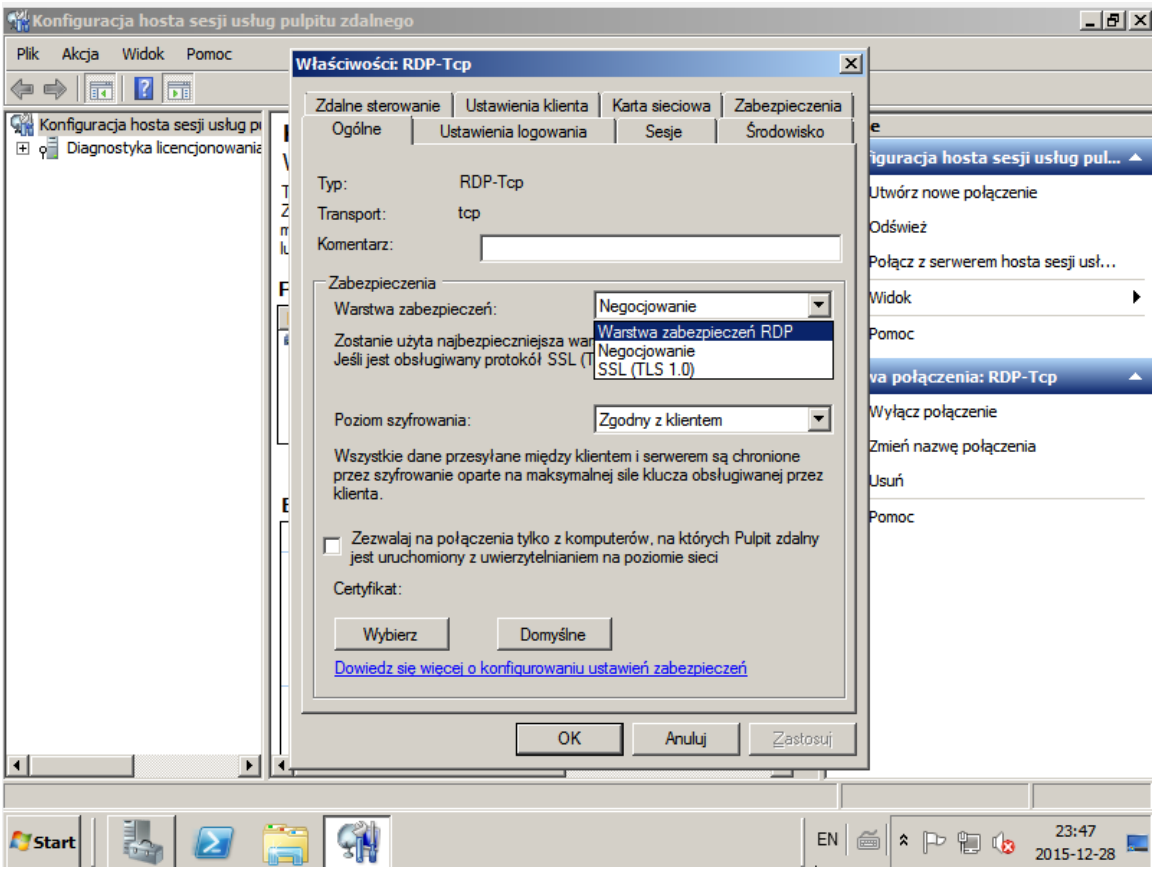
3. Przebieg ćwiczenia laboratoryjnego

W pierwszej kolejności skonfigurowano protokół TLS/SSL na maszynie z systemem Windows Server 2008.



Rys1. Zrzut ekranu z widoku Konfiguracji hosta sesji usług pulpitu zdalnego.

W drugiej kolejności z listy połączeń wybrano połączenie *RDP-Tcp* oraz typ połączenia *Microsoft RDP wersja.*



Rys2. Zrzut ekranu Właściwości RDP-Tcp.

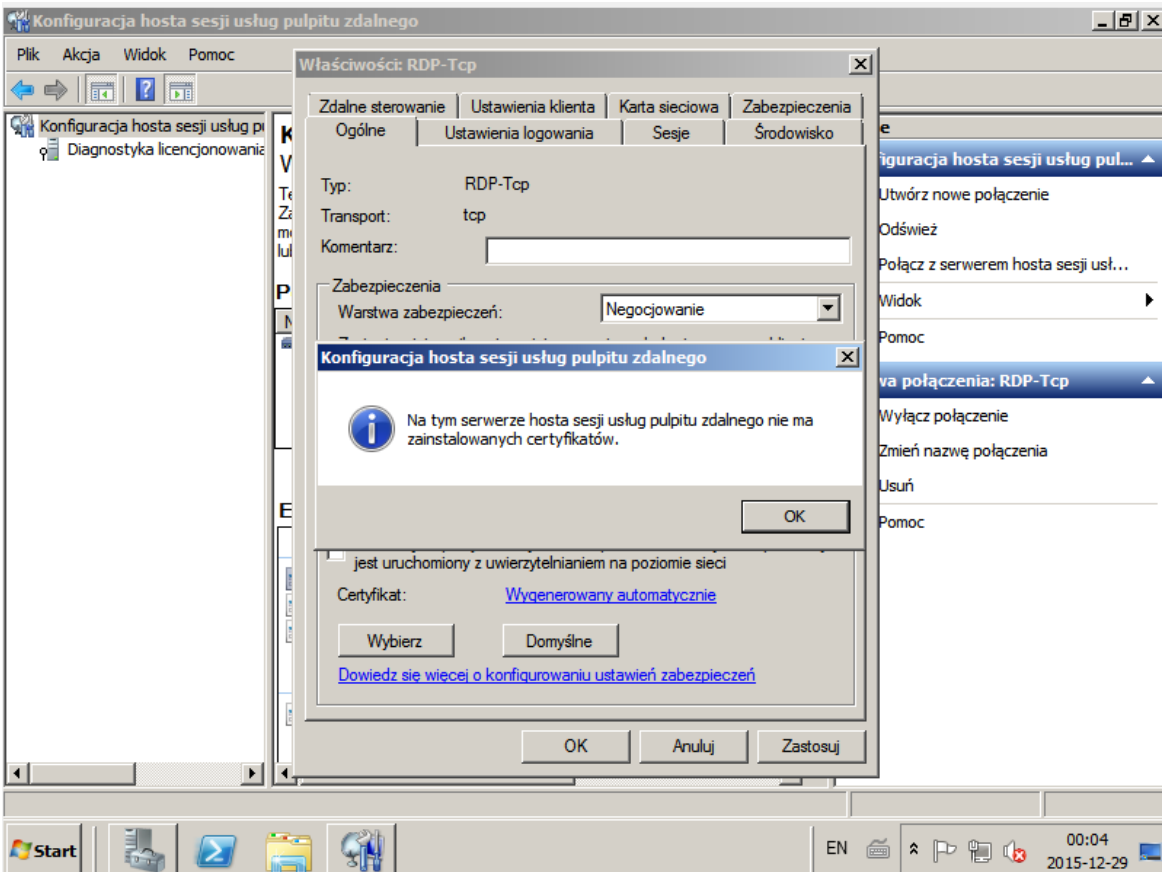
We właściwościach połączenia możemy ustalić *Warstwę zabezpieczeń*:

- Negocjowanie – zostanie użyta najbezpieczniejsza warstwa obsługiwana przez klienta. Jeśli jest obsługiwany protokół SSL (TLS 1.0), to zostanie on użyty.
- Zabezpieczenia RDP – komunikacja między serwerem, a klientem wykorzystujący szyfrowanie wg protokołu DRP.
- SSL (TSL 1.0) – będzie używany do uwierzytelnienia serwera oraz do szyfrowania wszystkich danych przesyłanych między serwerem, a klientem.

Możemy również ustalić poziom szyfrowania:

- Poziom niski – 56 bit.
- Zgodny z klientem.
- Poziom Wysoki – 128 bit.
- Zgodny z FISP.

Przy wyborze TLS/SSL jako warstwy zabezpieczeń należy wybrać z listy certyfikat wraz z kluczem prywatnym. Na potrzeby laboratorium wybrano certyfikat główny. W przypadku warunków rzeczywistych należy utworzyć osobną parę kluczy i podpisać je cyfrowo za pomocą odpowiedniego urzędu certyfikacji.



Rys3. Zrzut ekranu z komunikatem o braku zainstalowanego certyfikatu.

Następnie wyeksportowano certyfikat CA i przekazano do klientów. Na maszynach klienckich otworzono utworzone certyfikaty i zainstalowano certyfikaty.

Podczas laboratorium pokazane zostało również podpisywanie certyfikatu TLS / SSL. W tym celu utworzono plik (*Certificate Signing Request*) .csr, następnie w narzędziu *Certification Authority* za pośrednictwem klucza prywatnego podpisano go i utworzono. W *Ścieżce autoryzacji* znalazł się *nasz* certyfikat.

4. Wnioski

Na laboratorium został przedstawiony protokół TLS (SSL). Został on skonfigurowany na serwerze (*Windows Server 2008*). Został wyeksportowany do maszyn klienckich i zainstalowany.