Ćwiczenia laboratoryjne z przedmiotu Kryptografia i Bezpieczeństwo Danych

Temat: Uruchamianie stron HTTPS i szyfrowanych połączeń FTP na Windows 10 Pro

Autor: Sławomir Samolej

Wprowadzenie

1. Wszystkie witryny internetowe, w których następuje wymiana informacji z użytkownikiem powinny oferować szyfrowaną komunikację HTTPS. Stosowana jest tam rodzina algorytmów szyfrowania SSL/TLS oraz wymiana kluczy z zastosowaniem kryptografii klucza publicznego. Prawidłowo skonfigurowana witryna HTTPS powinna mieć zainstalowany certyfikat SSL uznany za wiarygodny. To znaczy, że dana firma potwierdza swoim autorytetem, że system szyfrowania jest wystawiony dla danego dostawcy strony przez uznawaną instytucję. Można zawsze „zapytać" się tej instytucji, czy korzystanie z systemu szyfrowanego połączenia jest przez nią uwiarygodnianie. Uruchomienie szyfrowanej strony polega na zainstalowaniu odpowiedniego certyfikatu w systemie oraz dokonaniu odpowiednich ustawień w konfiguracji serwera WWW.
2. Podobnie, jak w przypadku stron internetowych, można skonfigurować serwer FTP do udostępniania plików tylko w trybie szyfrowania transmisji. Podobnie, jak w przypadku serwera WWW do szyfrowania transmisji należy stosować uwiarygodniony certyfikat SSL.

Uwagi:

Ćwiczenie będzie polegało na uruchomieniu serwerów HTTPS i FTP z szyfrowanym transferem danych na platformie Windows 10 Pro. Okazuje się, że na potrzeby nieautoryzowanej szyfrowanej komunikacji można stworzyć w systemie Windows własne certyfikaty. Nie pozwalają one utrzymywanie wiarygodnych serwerów HTTPS/FTP z szyfrowaniem, ale umożliwiają zbudowanie odpowiedniej infrastruktury do uruchomienia i przetestowania serwisów. W dalszej kolejności można wystąpić o przydzielenie certyfikatów.

Przebieg ćwiczenia

1. Proszę prześledzić wprowadzenie prowadzącego dotyczące konfiguracji IIS w celu dostarczania stron z zastosowaniem protokołu HTTPS
2. Proszę prześledzić wprowadzenie prowadzącego dotyczące konfiguracji IIS w celu umożliwiania szyfrowanego dostępu do plików na serwerze FTP
3. Proszę zainstalować narzędzie WinCSP dostępne na stronie [3]. Jest to współczesne narzędzie do bezpiecznego transferu plików z innych komputerów i chmury.
4. Proszę samodzielnie skonfigurować na pojedynczym komputerze z systemem Windows 10 Pro IIS w celu dostarczania stron WWW i plików w sposób zaszyfrowany. Pomocne będą pozycje literatury [5], [1] i [2].
5. Proszę zastosować przeglądarkę do odwołania się do waszej szyfrowanej strony, oraz program CSP do ustanowienia chronionego połączenie FTP.
6. Proszę przeanalizować poradniki dotyczące instalacji Serwera SFTP/SSH z zastosowaniem OpenSSH na platformie Windows 10 oraz przetestować możliwość łączenia się z komputerem z zastosowaniem tego protokołu.

Literatura

[1] (Konfiguracja IIS do udostępniania stron HTTPS)
https://onlinehelp.coveo.com/en/ces/7.0/administrator/enabling_ssl_in_iis.htm

[2] (Konfiguracja IIS do tworzenia szyfrowanego połączenie FTP)
https://winscp.net/eng/docs/guide_windows_ftps_server

[3] (Strona narzędzia WinCSP)
https://winscp.net/eng/docs/lang:pl

[4] (Ogólne wprowadzenie do certyfikatów SSL)
https://wp-opieka.pl/blog/co-to-jest-ssl-i-dlaczego-nie-mozesz-sie-bez-niego-obejsc/?gclid=Cj0KCQjwzZj2BRDVARIsABs3l9IeXHpUzaNpLG7Jku0PT1ploZzhMv-unDcGbeKJT8uvzTcS4k9M3sEaAqAWEALw_wcB

[5] (Instalacja IIS) https://www.howtogeek.com/112455/how-to-install-iis-8-on-windows-8/