|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| Ochrona komunikacji |
| Cyberbezpieczeństwo, Laboratorium nr.9 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**1. Zadania i pytania (TLS)**

**Zadania 1.1-1.3;**

Przebieg zadań na zrzutach ekranu poniżej:

**Pytanie 1.4;**

Oba protokoły działają w głównej mierze tak samo (służą do szyfrowania i uwierzytelniania danych, aby chronić je przed odczytem przez osoby niepożądane), z tą różnicą że TLS jest następcą SSL, a więc wprowadza różnego rodzaju ulepszenia, między innymi w zakresie bezpieczeństwa i wydajności działania protokołu.

**Pytanie 1.5;**

TLS/SSL handshake to process negocjacji parametrów używanych do nawiązywania połączenia między klientem a serwerem. Podczas tego procesu następuje wymiana szczegółów połączenia takich jak wersja protokołu, klucze sesji czy użyte algorytmy szyfrujące. Jest niezbędnym elementem bezpiecznego przesyłania danych zaszyfrowaną drogą.

**Pytanie 1.6;**

Protokół TLS/SSL zapewnia ochronę transmisji danych poprzez ich szyfrowanie oraz uwierzytelnianie stron komunikacji. Zastosowania:

* Szyfrowanie połączenia między klientem a serwerem podczas przesyłania danych logowania przy rejestracji do wybranego serwisu (np. Netflix)
* Szyfrowanie połączenia między klientem a serwerem podczas prowadzenia połączenia głosowego przez aplikację typu Zoom (ochrona danych przed podsłuchem)
* Uwierzytelnianie stron internetowych HTTPS (np. facebook.com)
* Szyfrowanie e-maili (SMTP)
* Bezpieczne połączenie z serwerem VPN (ochrona prywatności)

**Pytanie 1.7;**  
TLS 1.2 i TLS 1.3. Wersja 1.3 uznawana jest obecnie jako standard i jest powszechnie używana w większości systemów.

**Pytanie 1.8;**

TLS 1.3, ponieważ eliminuje przestarzałe algorytmy (uwierzytelniania i szyfrowania), redukuje liczbę podatnych funkcji i usprawnia proces handshake.

**Pytanie 1.9;**

TLS 1.3, ponieważ korzysta z wydajniejszych algorytmów oraz sam proces przebiega szybciej (oraz zużywa mniej energii) ze względu na:

* 1-RTT zamiast 2-RTT
* AES zamiast asymetrycznego RSA
* Krótszy handshake (każda wymiana kluczy korzysta z Diffiego-Hellmana)

**Pytanie 1.10;**

Wireshark przechwycił obydwie wersje protokołu: TLS 1.2 oraz TLS 1.3

**Pytanie 1.11;**

Zwykle z: *ClientHello*, *ServerHello*, wymiany certyfikatów i kluczy sesji. Proces ten różni się w zależności od wersji protokołu:

* **TLS 1.2**:
  1. *ClientHello*: Klient wysyła informacje o obsługiwanych algorytmach szyfrowania, wersji protokołu i danych do wygenerowania klucza.
  2. *ServerHello*: Serwer odpowiada wyborem algorytmu i wersji TLS.
  3. *Certificate*: Serwer wysyła swój certyfikat do uwierzytelnienia.
  4. *Key Exchange*: Klient i serwer wymieniają dane pozwalające na ustalenie wspólnego klucza sesji.
  5. *Finished*: Obie strony kończą proces, potwierdzając poprawność ustaleń.
* **TLS 1.3**:
  1. *ClientHello*: Klient wysyła propozycję algorytmów szyfrowania i dane do wygenerowania klucza (w tym dane dla szyfrowania asymetrycznego).
  2. *ServerHello*: Serwer akceptuje algorytm i generuje klucz sesji na podstawie danych klienta. Certyfikat serwera jest przesyłany w jednym kroku, skracając czas wymiany.
  3. *Finished*: Po weryfikacji certyfikatu połączenie jest szyfrowane, co zmniejsza liczbę rund komunikacji.

**Pytanie 1.12;**

Zależy od wersji oprogramowania zarówno po stronie klienta jak i serwera (wsparcie systemowe oraz konfiguracja oprogramowania mają znaczenie). Z tego powodu warto regularnie aktualizować oprogramowanie aby mieć dostęp do najnowszych, najszybszych i najbezpieczniejszych wersji protokołów takich jak TLS. Proces komunikacji przebiegać będzie po najnowszej wspólnej wersji protokołu uzgodnionej w handshaku (obie strony muszą obsługiwać daną wersję). Dodatkowo administrator sieci może wymusić użycie konkretnej wersji protokołu. Niektóre przeglądarki lub aplikacje pozwalają na wymuszenie używania nowszych wersji. Serwery proxy lub urządzenia pośredniczące mogą wymuszać starsze wersje w przypadku braku wsparcia.

**2. Zadania (OpenVPN)**

**Zadania 2.1-2.4;**

Przebieg zadań na zrzutach ekranu poniżej:

**3. Zadania i pytania (OpenVPN)**

**Zadania 3.1-3.4;**

Przebieg zadań na zrzutach ekranu poniżej:

**Pytanie 3.5;**

Ataki

**Pytanie 3.6;**

Ataki

**Pytanie 3.7;**

Ataki

**4. Zadania i pytania**

**Zadania 4.1-4.3;**

Przebieg zadań na zrzutach ekranu poniżej:

**Pytanie 4.4;**

Ataki

**Pytanie 4.5;**

Ataki

**Pytanie 4.6;**

Ataki