LABORATORIUM BEZPIECZEŃSTWO TECHNOLOGII INFORMATYCZNYCH

Data wykonania ćwiczenia:	14.11.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	6

Temat: Analiza Certyfikatów SSL/TLS

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Cel zadania:

Zapoznanie się z analizą certyfikatów SSL/TLS używanych przez różne witryny internetowe oraz zidentyfikowanie informacji zawartych w certyfikatach i mechanizmów szyfrowania.

Wstęp teoretyczny

Certyfikaty SSL/TLS odgrywają kluczową rolę w zapewnianiu bezpieczeństwa komunikacji internetowej poprzez umożliwienie szyfrowania danych i potwierdzanie autentyczności witryny. Analiza tych certyfikatów pozwala na lepsze zrozumienie, jak witryny internetowe zarządzają bezpieczeństwem swojej komunikacji. W tym kontekście skupimy się na kilku kluczowych aspektach analizy certyfikatów SSL/TLS.

1. Właściciel i Organizacja: Certyfikaty SSL/TLS zawierają informacje o właścicielu, co obejmuje zarówno nazwę domeny, jak i organizację posiadającą certyfikat. Weryfikacja tych danych umożliwia użytkownikom potwierdzenie, czy komunikują się z wiarygodnym źródłem.

2. Mechanizmy Szyfrowania: Analiza certyfikatów pozwala na zidentyfikowanie używanych mechanizmów szyfrowania. Znajomość algorytmów, długości klucza i innych parametrów umożliwia ocenę poziomu bezpieczeństwa komunikacji.

3. Protokoły SSL/TLS: Sprawdzanie obsługiwanych protokołów SSL/TLS jest kluczowe dla zapewnienia, że witryna korzysta z aktualnych standardów bezpieczeństwa. Unikanie przestarzałych protokołów redukuje ryzyko ataków.

4. Ważność Certyfikatu: Termin ważności certyfikatu wpływa na trwałość zabezpieczeń. Analiza pozwala ocenić, czy witryna regularnie odnawia swoje certyfikaty, co jest kluczowe dla utrzymania bezpiecznej komunikacji.

5. Porównanie z Innymi Witrynami: Porównywanie certyfikatów różnych witryn pozwala na zrozumienie, w jaki sposób różne instytucje zarządzają swoim bezpieczeństwem. To umożliwia wyciąganie wniosków dotyczących najlepszych praktyk.

Wybór witryn i analiza plików cookies

Witryna 1.

Jako pierwszą wybierzemy naszą uczelnianą witrynę e-uczelni pod adresem *https://e-uczelnia.ath.bielsko.pl*.

Nazwa właściciela: *.ath.bielsko.pl
Organizacja: Akademia Techniczno Humanistyczna w Bielsku Białej
Ważność certyfikatu: 20.01.2024
Algroytmy szyfrowania: PKCS #1 SHA-384 With RSA Encryption

Widzimy że algorytm składa się z kilku fragmentów.

- PKCS #1 - (Public Key Cryptography Standards #1)
- SHA-384 - jest to hashująca funkcja kryptograficzna, która generuje 384 bitowe pole za pomocą którego wpływa na zwiększenie bezpieczeństwa witryny
- RSA Encryption - jest to asymetryczny algorytm kodujący wykorzystywany do bezpiecznego przekazywania danych

Następnym krokiem jest analiza protokołów SSL/TLS, zrobimy to za pomocą windowse powershella i funkcji OpenSSL.

Po skonfigurowaniu OpenSSL możemy zauważyć że powyższa witryna korzysta z poniższych protokołów:

```
New, TLSv1.2, Cipher is DHE-RSA-AES256-GCM-SHA384
```

1. New: Jest to informacja o rozpoczęciu nowego połączenia z serwerem.
2. TLSv1.2: Oznacza, że używany jest protokół TLS w wersji 1.2. TLS (Transport Layer Security) jest protokołem kryptograficznym używanym do zapewnienia bezpieczeństwa komunikacji w Internecie. Wersja 1.2 jest starszą wersją protokołu, która oferuje pewien poziom zabezpieczeń.
3. Cipher is DHE-RSA-AES256-GCM-SHA384: Zawiera informacje o używanej metodzie szyfrowania (cipher), która w tym przypadku jest DHE-RSA-AES256-GCM-SHA384.
    - DHE-RSA: Oznacza metodę wymiany kluczy (Diffie-Hellman Exchange z podpisem cyfrowym opartym na algorytmie RSA), która jest używana do bezpiecznej wymiany kluczy.
    - AES256-GCM: Jest to algorytm szyfrowania (Advanced Encryption Standard) z kluczem 256-bitowym w trybie Galois/Counter Mode (GCM), który zapewnia szyfrowanie danych.
    - SHA384: Jest to funkcja skrótu (Secure Hash Algorithm) o długości 384 bitów, która jest używana do zabezpieczenia integralności danych.

Powyższe protokoły są dość klasyczne i wszechobecne, więc możemy założyć że są bezpieczne, aczkolwiek istnieje nowsza i bezpieczniejsza wersja protokołu TLSv1.3

Witryna 2

Jako drugą witrynę wybrałem swoją własną stronę internetową *https://igorgawlowicz.pythonanywhere.com*.

Strona ta korzysta z bazowych zabezpieczeń witryny matki **.pythonanywhere.com*.

Nazwa właściciela: *.pythonanywhere.com
Organizacja:
Ważność certyfikatu: 07.01.2024
Algroytmy szyfrowania: PKCS #1 SHA-256 With RSA Encryption

Widzimy że algorytm składa się z kilku fragmentów.

- PKCS #1 - (Public Key Cryptography Standards #1)
- SHA-256 - jest to hashująca funkcja kryptograficzna, w odróżnieniu od SHA-384 z poprzedniej witryny jest to nieco mniej bezpieczna opcja, jednak korzystanie nawet z 256 bitów jest zazwyczaj wystarczającym zabezpieczniem.
- RSA Encryption - jest to asymetryczny algorytm kodujący wykorzystywany do bezpiecznego przekazywania danych

Analiza protokołów SSL/TLS

```
TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
```

1. TLSv1.3: Oznacza, że używany jest protokół TLS w wersji 1.3. TLS (Transport Layer Security) jest protokołem kryptograficznym używanym do zapewnienia bezpieczeństwa komunikacji w Internecie.

Reszta uwzględniona już w Witryna 1

Witryna 3

Kolejną witryną będzie *https://thesecmaster.com*.

Jest to strona na, której znalazłem instrukcje instalacji modułu OpenSSL.

Nazwa właściciela: thesecmaster.com
Organizacja: Cloudflare, Inc.
Ważność certyfikatu: 01.07.2024
Algroytmy szyfrowania: X9.62 ECDSA Signature with SHA-256

Widzimy że algorytm składa się z kilku fragmentów.

- X9.62: Jest to standard określający algorytmy do krzywych eliptycznych, a także metody generowania kluczy, sygnatury cyfrowej i wymiany kluczy w publicznych systemach kryptograficznych.
- ECDSA (Elliptic Curve Digital Signature Algorithm): Jest to algorytm podpisywania cyfrowego oparty na krzywych eliptycznych. Wykorzystuje one matematyczne właściwości krzywych eliptycznych do generowania kluczy oraz sygnatur cyfrowych, co umożliwia bezpieczne przeprowadzanie operacji kryptograficznych.
- SHA-256: Jest to funkcja skrótu z rodziny algorytmów Secure Hash Algorithm, która generuje skrót (hasz) o długości 256 bitów z dowolnie długiego ciągu danych wejściowych. SHA-256 jest powszechnie używaną funkcją skrótu, która zapewnia wysoki poziom bezpieczeństwa.

Analiza protokołów SSL/TLS

```
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
```

Wynik bardzo podobny do pierwszej witryny z różnicą w postaci nowszej wersji TLS. Witryna 1

Witryna 4

Następną witryną będzie *https://slproweb.com*.

Jest to strona, z której pobrałem instalator modułu OpenSSL

Nazwa właściciela: slproweb.com
Organizacja:

Ważność certyfikatu: 17.01.2024
Algroytmy szyfrowania: PKCS #1 SHA-256 With RSA Encryption

Zastosowane tutaj algorytmy były poruszone już wcześniej.

Analiza protokołów SSL/TLS

```
TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
```

Wynik identyczny jak w drugiej witrynie. Witryna 2

Witryna 5

Ostatnią witryną będzie platforma służąca jako biblioteka gier *https://store.steampowered.com*

Nazwa właściciela: store.steampowered.com
Organizacja: Valve Corp
Ważność certyfikatu: 17.12.2023
Algroytmy szyfrowania: PKCS #1 SHA-256 With RSA Encryption

Zastosowane tutaj algorytmy były poruszone już wcześniej.

Analiza protokołów SSL/TLS

```
TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
```

Wynik identyczny jak w drugiej witrynie. Witryna 2

Wnioski

1. Właściciel i Organizacja:

- Wnioskując z analizy certyfikatów, można ustalić właścicieli i związane z nimi organizacje. Zaufane witryny internetowe prezentują certyfikaty z jasno zidentyfikowanymi informacjami na temat właściciela, co buduje zaufanie użytkowników.
-

2. Mechanizmy Szyfrowania:

- Algorytmy szyfrowania używane w certyfikatach są kluczowe dla bezpieczeństwa komunikacji. Zauważono, że większość witryn wykorzystuje silne algorytmy szyfrowania, takie jak AES-256-GCM, co sugeruje wysoki poziom bezpieczeństwa.

3. Protokoły SSL/TLS:

- Analiza protokołów SSL/TLS pokazuje, że większość zbadanych witryn korzysta z najnowszej wersji TLSv1.3, co świadczy o ich dążeniu do zapewnienia najwyższego poziomu bezpieczeństwa w komunikacji.

4. Ważność Certyfikatów:

- Data ważności certyfikatów ma istotne znaczenie dla trwałości zabezpieczeń. Większość analizowanych witryn posiada ważne certyfikaty, co świadczy o ich dbałości o utrzymanie bezpiecznej komunikacji.

5. Porównanie Praktyk Bezpieczeństwa:

- Porównanie certyfikatów różnych witryn pozwala na zrozumienie różnic w podejściu do bezpieczeństwa. Witryny korzystające z nowszych wersji protokołów i silniejszych algorytmów prezentują się jako bardziej bezpieczne.