Infrastruktura klucza publicznego i protokół TLS

Paweł Topa

18 marca 2025

1 Stworzenie i konfiguracja `Centrum Certyfikacji`

Do stworzenia `CA` nie są wymagane uprawnienia administratorskie, jednak tak będzie nam wygodniej gdyż później konieczna będzie konfiguracja serwera `httpd` do której wymagane będą takie uprawnienia.

- ☐1 Prześledź zawartość domyślnego pliku konfiguracyjnego narzędzi `OpenSSL` – `/etc/ssl/openssl.cnf`[1] ze szczególnym uwzględnieniem drzewa katalogów, w którym to będą umieszczane generowane pliki i w razie potrzeby dokonaj odpowiednich zmian. Wpisz również domyślne wartości dotyczące parametrów tworzonego `CA` i późniejszych certyfikatów.
- ☐2 Utwórz w odpowiedniej lokalizacji (zgodnej z wpisem w pliku `openssl.cnf`) plik tekstowy o nazwie `serial` i umieść w nim numer seryjny dla tworzonych certyfikatów — zaczniemy od 01.
- ☐3 Utwórz pusty plik tekstowy o nazwie `index.txt`, w którym będą przechowywane informacje o podpisanych certyfikatach. Jego lokalizacja musi być zgodna z tym, co ustawione jest w pliku konfiguracyjnym.
- ☐4 Utwórz (używając polecenia `openssl`) podpisany przez samego siebie (`selfsigned`) certyfikat i klucz prywatny dla **Centrum Certyfikacji** `CA`[2], którego ważność będzie 10 lat. Ustal nazwy plików na odpowiednio `ca.crt` i `ca.key`.
- ☐5 Wypisz zawartość certyfikatu `CA` posługując się opcją `text` dla polecenia `openssl` oraz wyświetl zawartość zarówno certyfikatu jak i klucza prywatnego jako pliku tekstowego.
- ☐6 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania .....

2 Stworzenie certyfikatu dla serwera `https`

- ☐1 Przejdź do innego katalogu (np. domowy katalog użytkownika `root`) i stwórz w nim zgłoszenie certyfikacji, które później zostanie podpisane przez `CA` oraz wykorzystane jako certyfikat serwera `http`[3]. CN powinno mieć inną wartość niż CN ustalone dla CA. Ustal nazwy tworzonych plików na `server.req` i `server.key` oraz ważność certyfikatu na 5 lat. Nie wymagaj podania hasła do szyfrowania klucza prywatnego, ponieważ będzie go trzeba podawać przy każdym uruchomieniu serwera `http`.
- ☐2 Wypisz zawartość zgłoszenia używając polecenia `openssl`.
- ☐3 Dokonaj podpisania zgłoszenia przez `CA` tworząc certyfikat w pliku `server.crt`.
- ☐4 Wypisz zawartość otrzymanego certyfikatu używając polecenia `openssl` i zwróć uwagę na pole opisujące wystawcę.
- ☐5 Obejrzyj zawartość plików przechowujących informacje o bazie certyfikatów: `serial` i `index.txt`
- ☐6 Dokonaj walidacji/weryfikacji wygenerowanego certyfikatu.
- ☐7 Wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania .....

[1] Specyficznie dla Kali Linux
[2] Certyfikat CA jest tzw certyfikatem *Root* i z oczywistych względów musi być podpisany przez własny klucz prywatny
[3] Pole `Organization Name` musi być takie same jak podane przy tworzeniu `CA`

3 Konfiguracja serwera `http` do współpracy z `OpenSSL`

☐1 Uruchom serwer `apache2` sprawdź czy strona serwera jest widoczna w przeglądarce

```
sudo systemctl start apache2.service
sudo systemctl status apache2.service
```

☐2 Skopiuj pliki `server.crt` i `server.key` do katalogu `/etc/apache2`

☐3 Włącz obsługę protokołu SSL:

```
sudo a2enmod ssl
```

☐4 Skonfiguruj stronę serwera dla protokołu HTTPS:

```
sudo a2ensite default-ssl
```

☐5 Popraw w pliku konfiguracyjnym `/etc/apache2/sites-enabled/default-ssl.conf` ścieżki do plików certyfikatu i klucza serwera.

☐6 Uruchom ponownie serwer `http`.

```
sudo systemctl restart apache2
```

☐7 Otwórz przeglądarkę i połącz się z serwerem przez protokół `https`.

☐8 Zwróć uwagę na szczegółowe informacje dotyczące certyfikatu

4 Komunikacja między klientem (przeglądarką) i serwerem HTTPS

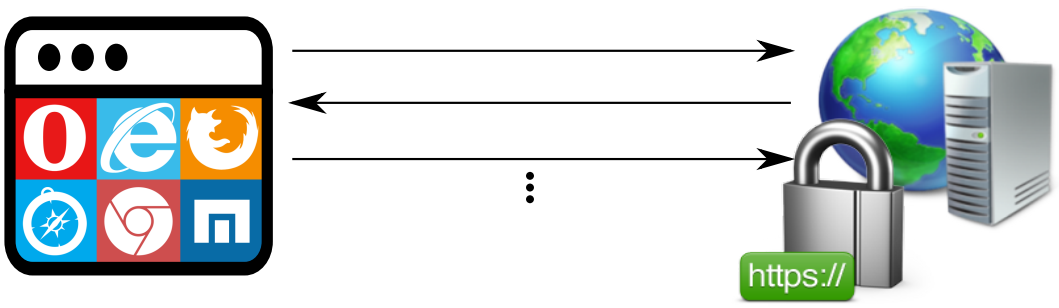
☐1 Uruchom sniffera o nazwie `wireshark` (na kliencie lub serwerze, potrzebne są uprawnienia administratora)

☐2 Zastosuj filtr aby widoczne były wyłącznie pakiety protokołu `ssl`

☐3 Znajdź pakiety jakie wymieniły ze sobą serwer i klient. Zlokalizuj fazę handshake i później fazę transmisji danych. Obejrzyj ich zawartość.

☐4 Znajdź w internecie opis poszczególnych komunikatów jakie zaobserwowałeś podczas badań.

☐5 Zwróć uwagę na poziom bezpieczeństwa zapewniany przez konfigurację (ustawienia konfiguracji mające wpływ na wybierane protokoły i algorytmy kryptograficzne). Zmodyfikuj konfigurację tak by zapewniała wysoki poziom bezpieczeństwa nawet kosztem kompatybilności.



5 Zaliczenie ćwiczenia

Zapisz do pliku kluczowe komendy zastosowane w celu wykonania ćwiczenia. Zapisz do pliku utworzone certyfikaty. Zapisz ostateczne wersje plików konfiguracyjnych serwera. Wszystko razem dołącz do odpowiedzi na zadanie w Teams.