Politechnika Białostocka

Sprawozdanie z pracowni specjalistycznej

Bezpieczeństwo Sieci Komputerowych

Ćwiczenie numer: 1

Temat: **Serwer HTTPS**

Wykonujący ćwiczenie:

Paweł Orzel

Łukasz Hossa

Kacper Seweryn

Studia dzienne

Kierunek: Informatyka

Semestr: VI

Grupa zajęciowa: Grupa PS 10

Prowadzący ćwiczenie: mgr inż. Katarzyna Borowska

Data wykonania ćwiczenia:28.02.2022

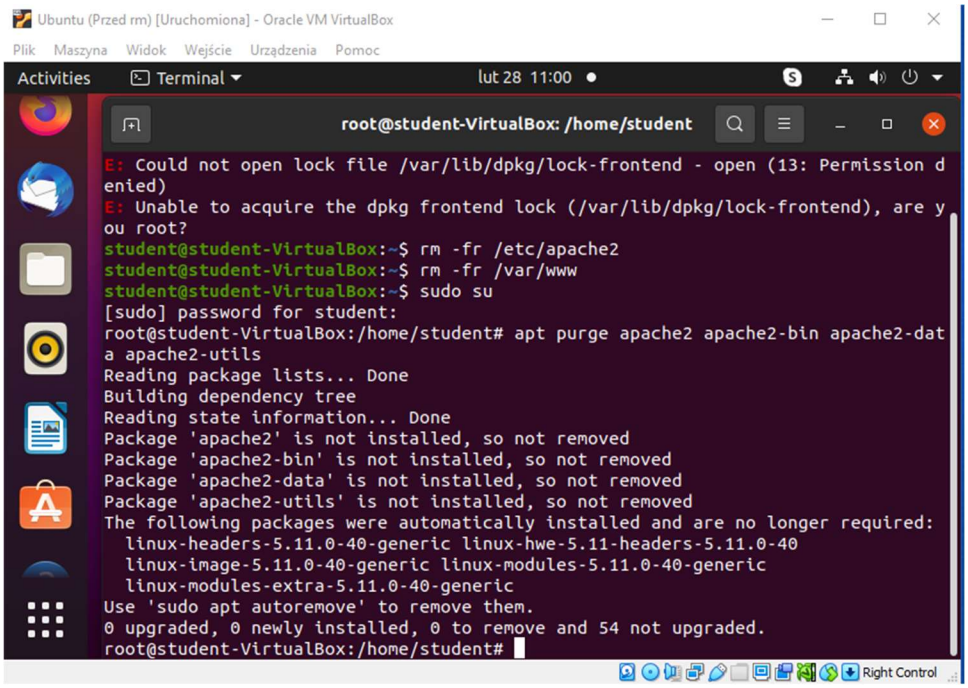
1. Teoria

HTTPS jest bezpieczną wersją protokołu http, której przeznaczeniem jest szyfrowanie danych wysyłanych między klientem, a serwerem. Dzięki protokołowi użytkownik może w bezpieczny sposób skorzystać z witryny. Protokół szyfruje danę za pomocą certyfikatu SSL, w momencie połączenia są ustalane klucze szyfrujące. Strona objęta protokołem https jest oznaczona poprzez kłódkę przy adresie strony.

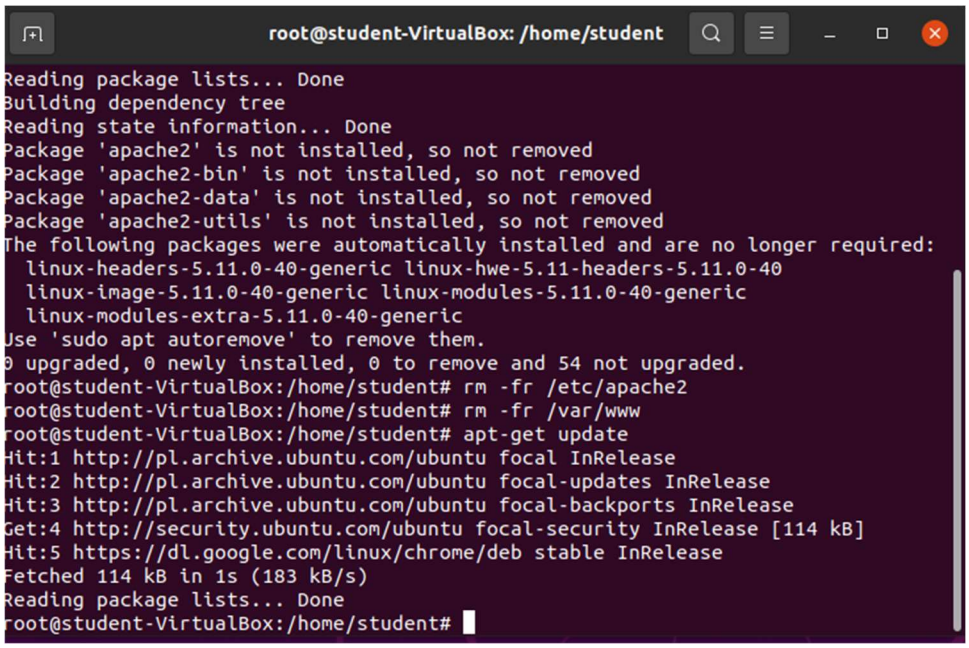
2. Realizacja zadania

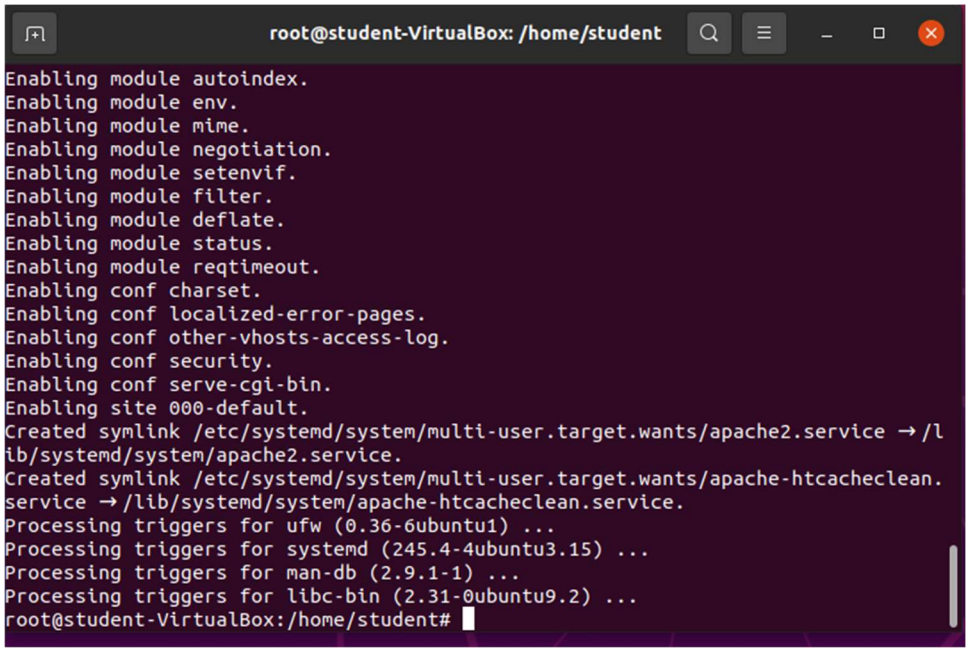
2.1 Deinstalacja starego pakietu

Deinstalacja ma zapobiec konfliktowi między ustawieniami ustawionymi przez poprzednich użytkowników systemu.



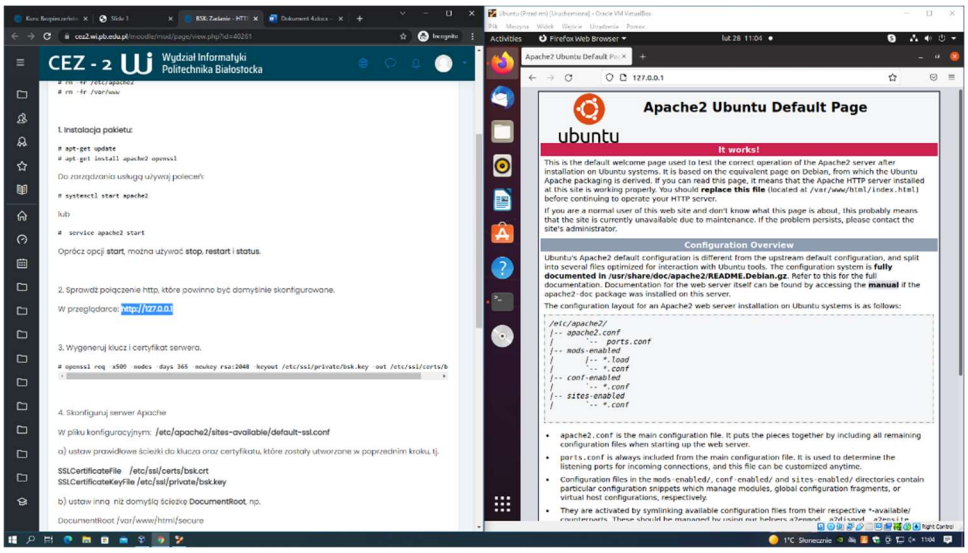
2.2 Instalacja pakietu





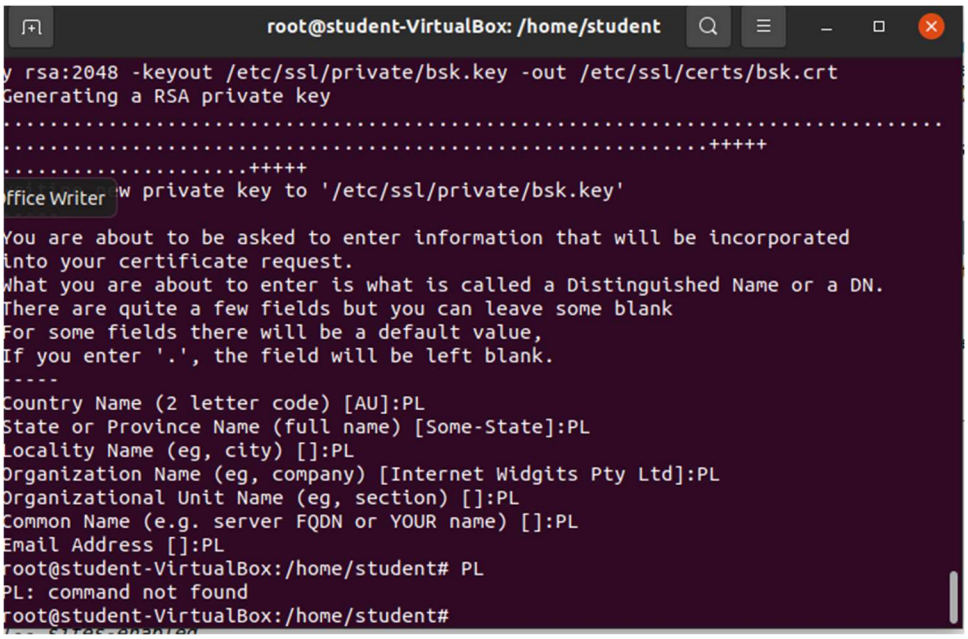
2.3 Sprawdź połączenie http, które powinno być domyślnie skonfigurowane

Sprawdzamy czy połączenie jest chronione protokołem http



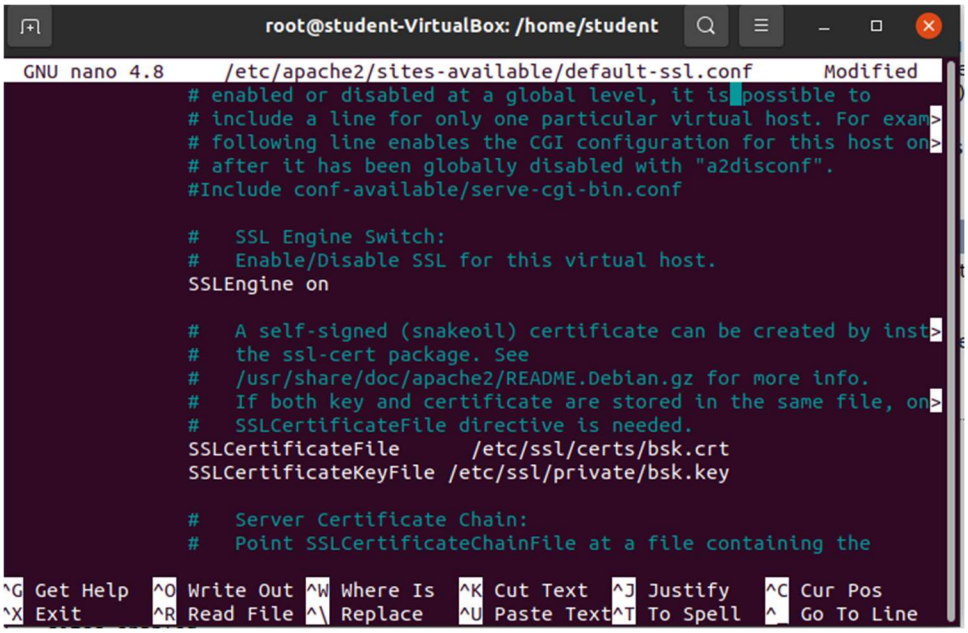
2.4-2.5 Wygeneruj klucz i certyfikat serwera oraz skonfiguruj serwer Apache

Plik CSR niezbędny jest do złożenia zamówienia i wystawienia certyfikatu SSL dla domeny. Następnie przesyłany jest do instytucji certyfikującej w celu jego podpisania, czyli utworzenia właściwego klucza publicznego dla certyfikatu SSL. Z tego właśnie powodu wygenerowanie pliku CSR jest niezbędne podczas rejestracji certyfikatu SSL



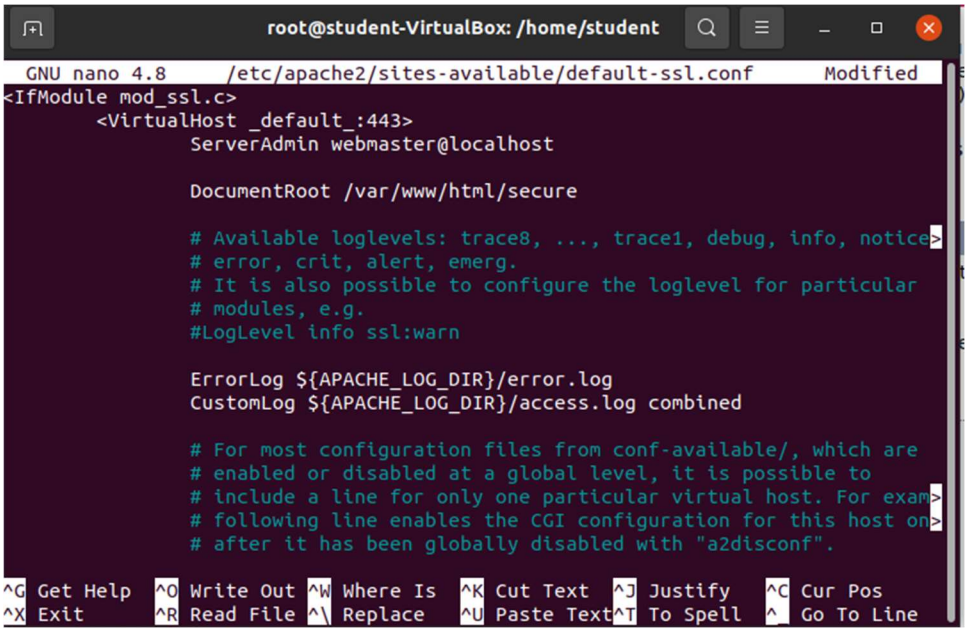
2.6. ustaw prawidłowe ścieżki do klucza oraz certyfikatu, które zostały utworzone w poprzednim kroku

Ustalona ścieżka dla certyfikatu : etc/ssl/certs/bsk.crt oraz dla klucza: etc/ssl/private/bsk.key

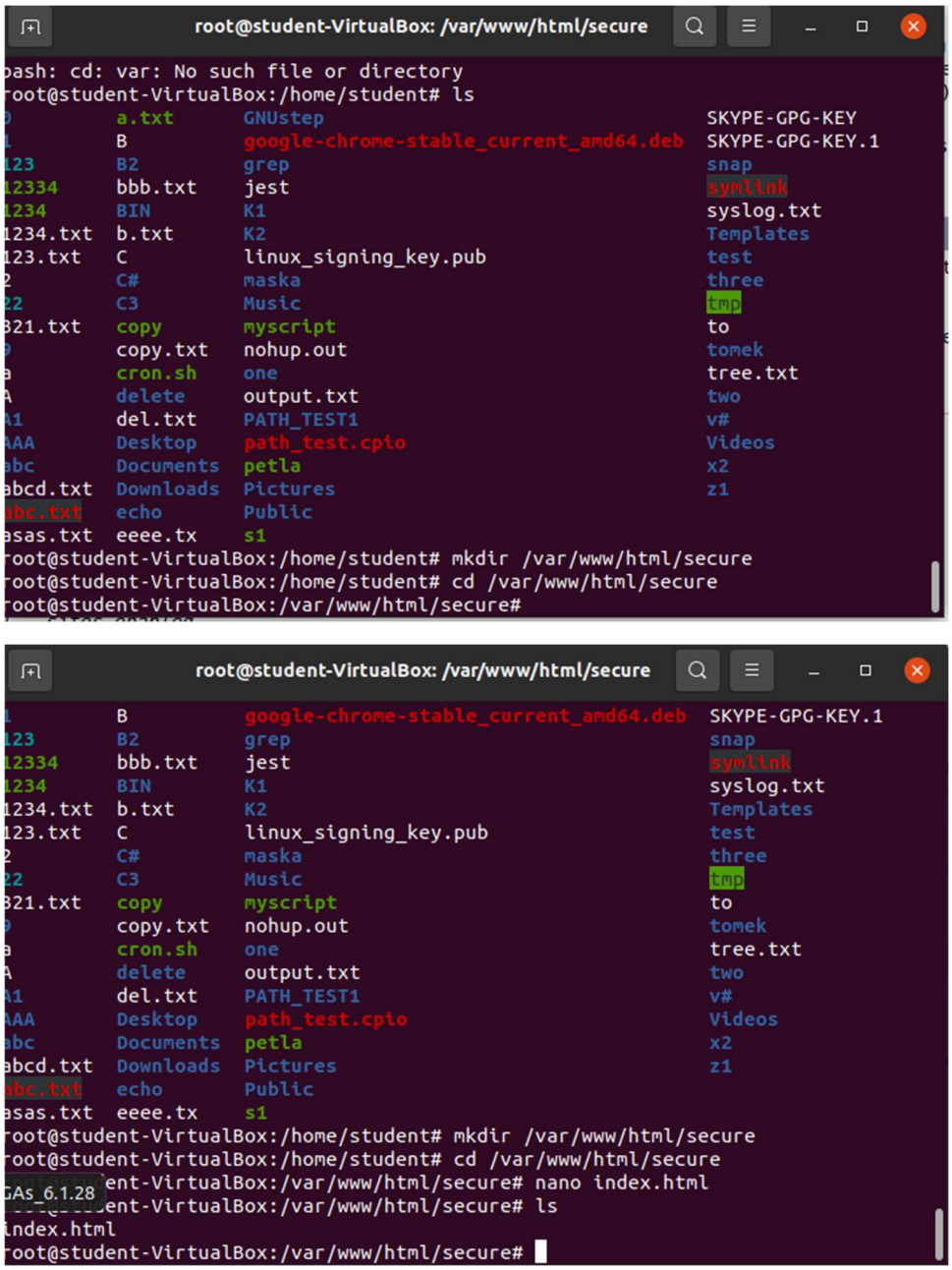


2.7. ustaw inną niż domyślą ścieżkę DocumentRoot

Zmiana ścieżki na /var/www/html/secure

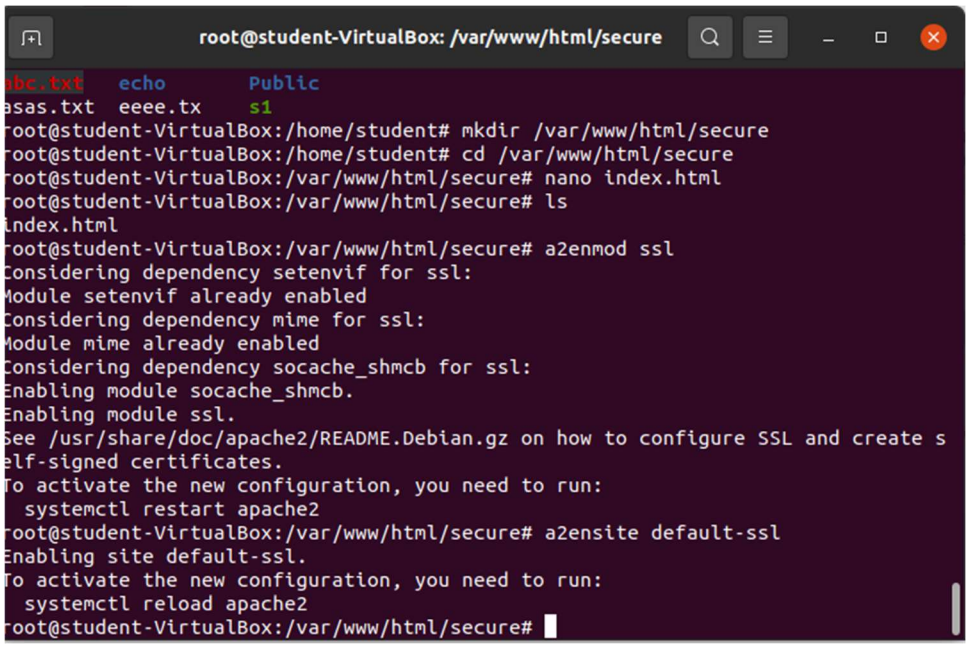


2.8. Utwórz w systemie katalog, który został wskazany jako DocumentRoot oraz utwórz w nim plik index.html z zawartością "Hello secure world".



2.9. Załaduj moduł ssl serwera Apache.

Domyślnie moduł ssl jest włączony, ale na wszelki wypadek należy włączyć ten moduł.



2.10. Zrestartuj serwer i sprawdź połączenie.

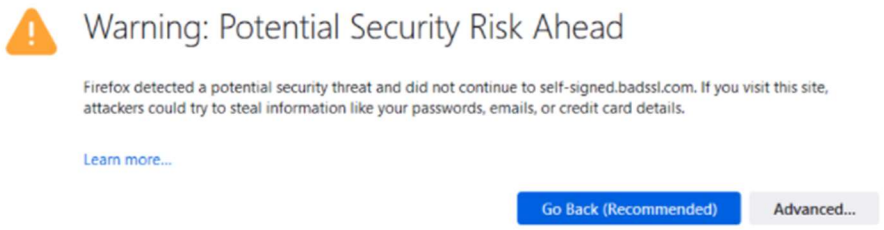
Po zresetowaniu i poprawnym skonfigurowaniu serwera oraz ustawieniu poprawnych ścieżek nasz adres https://127.0.0.1 powinien być zabezpieczony poprzez widoczną kłódkę przy adresie

3. Wnioski

Niezbędnym elementem protokołu https jest wygenerowanie klucza i certyfikatu, dzięki temu jesteśmy w stanie poprawnie zabezpieczyć naszą stronę. Jeśli domena jest odpowiednia skonfigurowana tj. ścieżki do wygenerowanego klucza oraz certyfikatu są poprawnie ustawione i posiada certyfikat SSL widoczna jest kłódka przy adresie naszej strony

Czy przeglądarka ostrzega użytkownika o niebezpiecznym połączeniu, mimo, że jest to HTTPS? Dlaczego? Jaki komunikat jest prezentowany? Co należałoby zrobić, aby go nie było?

Jeśli certyfikat nie może zostać zweryfikowany lub szyfrowanie jest zbyt stare zostanie wtedy wyświetlony komunikat o potencjalnym ryzyku:



Przeglądarka nie będzie nas ostrzegać w przypadku, gdy certyfikat będzie podpisany przez instytucję zaufaną, której klucz publiczny zapisany jest w przeglądarce.