

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

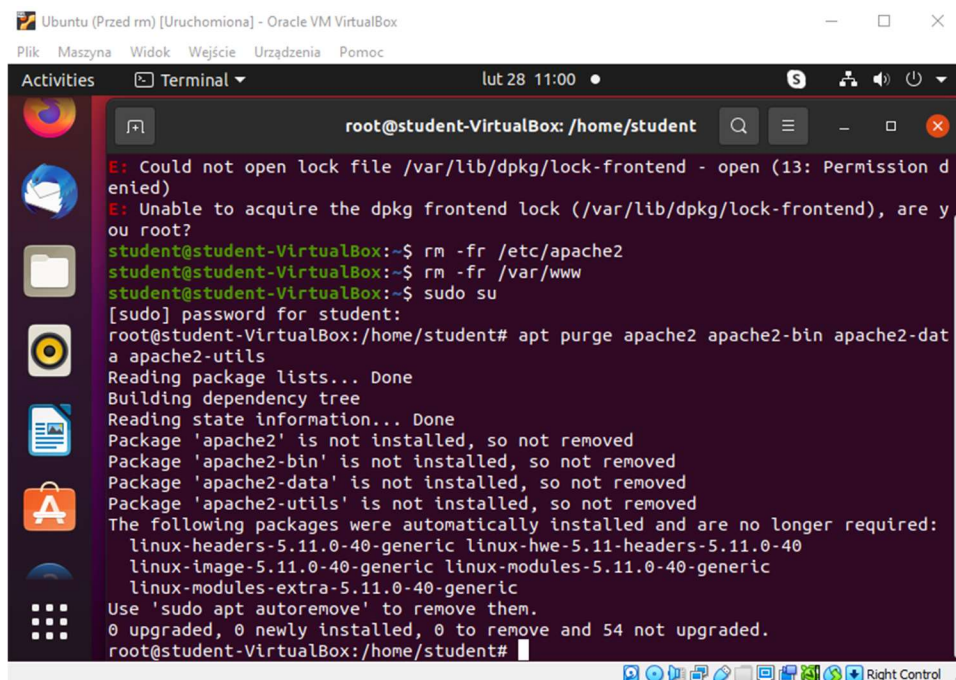
1. Teoria

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 daną 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.



```
Ubuntu (Przed rm) [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Activities Terminal lut 28 11:00
root@student-VirtualBox: /home/student
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?
student@student-VirtualBox:~$ rm -fr /etc/apache2
student@student-VirtualBox:~$ rm -fr /var/www
student@student-VirtualBox:~$ sudo su
[sudo] password for student:
root@student-VirtualBox:/home/student# apt purge apache2 apache2-bin apache2-data apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'apache2' is not installed, so not removed
Package 'apache2-bin' is not installed, so not removed
Package 'apache2-data' is not installed, so not removed
Package 'apache2-utils' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-40-generic linux-hwe-5.11-headers-5.11.0-40
  linux-image-5.11.0-40-generic linux-modules-5.11.0-40-generic
  linux-modules-extra-5.11.0-40-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 54 not upgraded.
root@student-VirtualBox:/home/student#
```

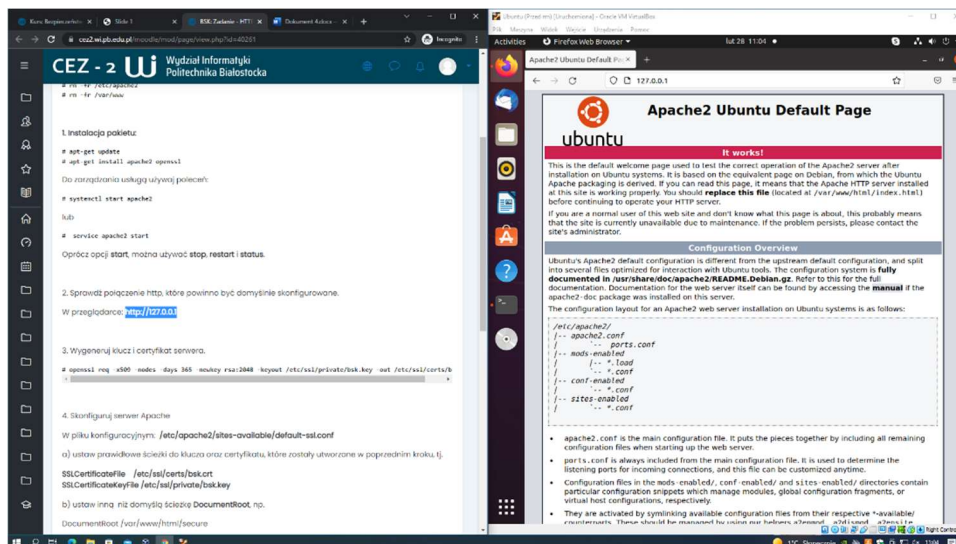
2.2 Instalacja pakietu

```
root@student-VirtualBox: /home/student
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'apache2' is not installed, so not removed
Package 'apache2-bin' is not installed, so not removed
Package 'apache2-data' is not installed, so not removed
Package 'apache2-utils' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-40-generic linux-hwe-5.11-headers-5.11.0-40
  linux-image-5.11.0-40-generic linux-modules-5.11.0-40-generic
  linux-modules-extra-5.11.0-40-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 54 not upgraded.
root@student-VirtualBox:/home/student# rm -fr /etc/apache2
root@student-VirtualBox:/home/student# rm -fr /var/www
root@student-VirtualBox:/home/student# apt-get update
Hit:1 http://pl.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://pl.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://pl.archive.ubuntu.com/ubuntu focal-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:5 https://dl.google.com/linux/chrome/deb stable InRelease
Fetched 114 kB in 1s (183 kB/s)
Reading package lists... Done
root@student-VirtualBox:/home/student#
```

```
root@student-VirtualBox: /home/student
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36-6ubuntu1) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
root@student-VirtualBox:/home/student#
```

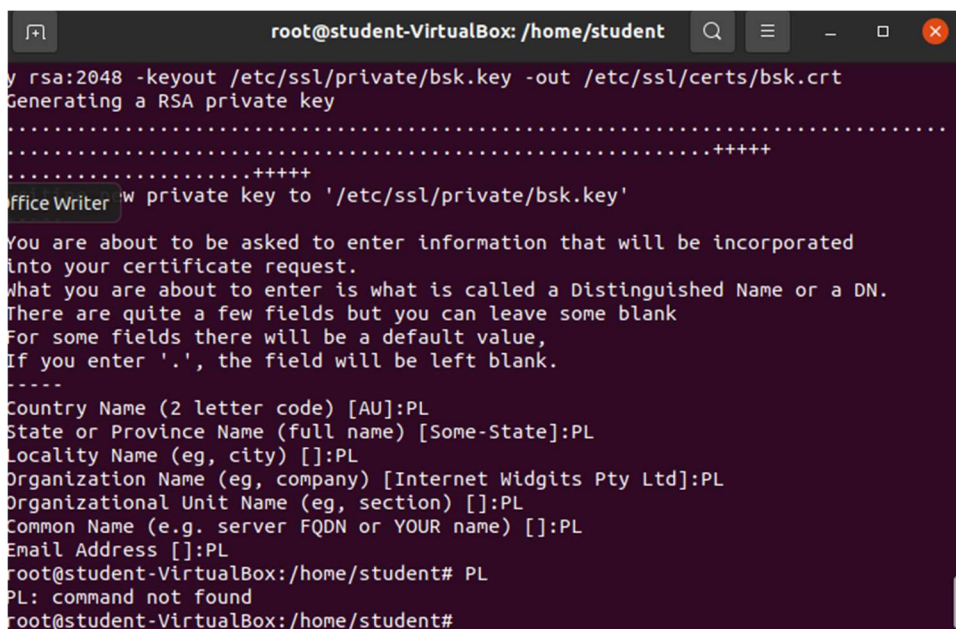
2.3 Sprawdź połączenie http, które powinno być domyślnie skonfigurowane

Sprawdzamy czy połączenie jest chronione protokołem http



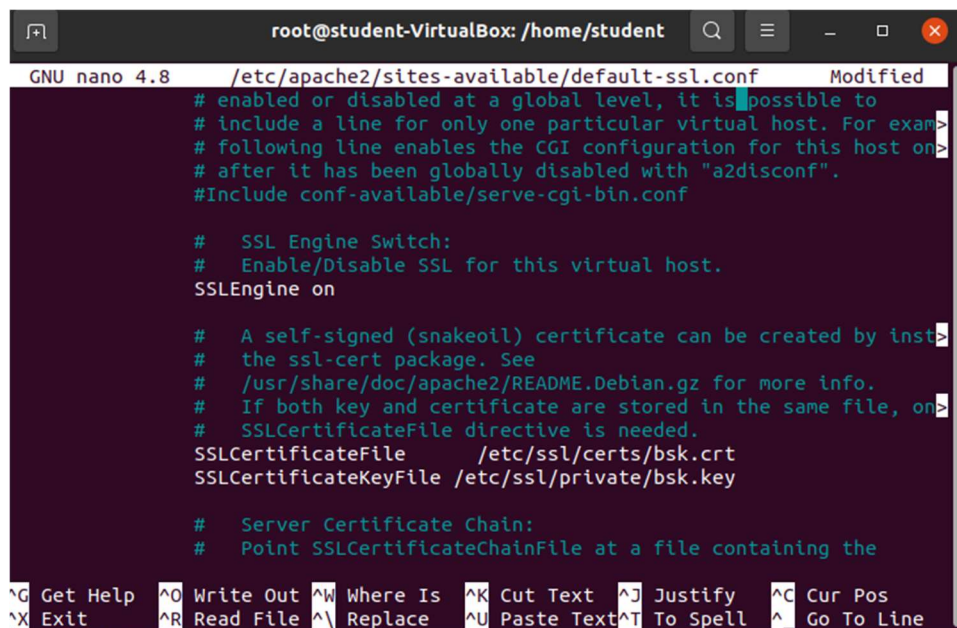
2.4-2.5 Wygeneruj klucz i certyfikat serwera oraz skonfiguruj serwer Apache

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



```
root@student-VirtualBox: /home/student
GNU nano 4.8 /etc/apache2/sites-available/default-ssl.conf Modified
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For exam>
# following line enables the CGI configuration for this host on>
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

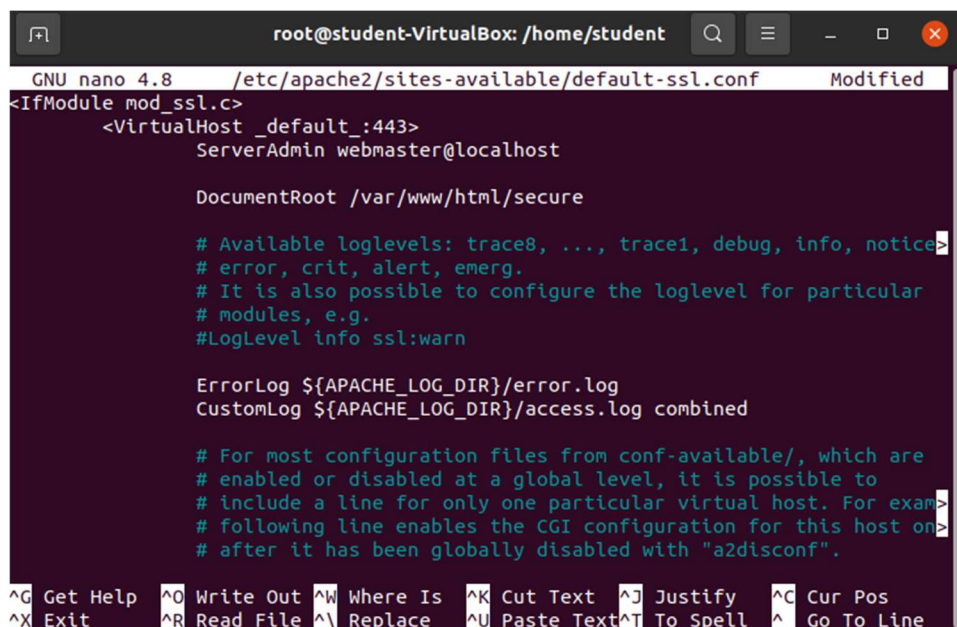
# A self-signed (snakeoil) certificate can be created by inst>
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, on>
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/bsk.crt
SSLCertificateKeyFile /etc/ssl/private/bsk.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

2.7. ustaw inną niż domyślną ścieżkę DocumentRoot

Zmiana ścieżki na /var/www/html/secure



```
root@student-VirtualBox: /home/student
GNU nano 4.8 /etc/apache2/sites-available/default-ssl.conf Modified
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html/secure

    # Available loglevels: trace8, ..., trace1, debug, info, notice>
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For exam>
    # following line enables the CGI configuration for this host on>
    # after it has been globally disabled with "a2disconf".
```

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

```
root@student-VirtualBox: /var/www/html/secure
bash: cd: var: No such file or directory
root@student-VirtualBox:/home/student# ls
a.txt      GNUstep      SKYPE-GPG-KEY
B          google-chrome-stable_current_amd64.deb SKYPE-GPG-KEY.1
123       B2          grep        snap
12334    bbb.txt     jest        symlink
1234     BIN        K1          syslog.txt
1234.txt b.txt      K2          Templates
123.txt  C          linux_signing_key.pub test
2        C#         maska       three
22       C3         Music       tmp
321.txt  copy       myscript    to
9        copy.txt   nohup.out   tomek
a        cron.sh    one         tree.txt
A        delete     output.txt  two
11       del.txt    PATH_TEST1  v#
AAA      Desktop    path_test.cpio Videos
abc      Documents  petla       x2
abcd.txt Downloads  Pictures    z1
abc.txt  echo       Public
asas.txt eeee.tx    s1

root@student-VirtualBox:/home/student# mkdir /var/www/html/secure
root@student-VirtualBox:/home/student# cd /var/www/html/secure
root@student-VirtualBox:/var/www/html/secure#
```

```
root@student-VirtualBox: /var/www/html/secure
B          google-chrome-stable_current_amd64.deb SKYPE-GPG-KEY.1
123       B2          grep        snap
12334    bbb.txt     jest        symlink
1234     BIN        K1          syslog.txt
1234.txt b.txt      K2          Templates
123.txt  C          linux_signing_key.pub test
2        C#         maska       three
22       C3         Music       tmp
321.txt  copy       myscript    to
9        copy.txt   nohup.out   tomek
a        cron.sh    one         tree.txt
A        delete     output.txt  two
11       del.txt    PATH_TEST1  v#
AAA      Desktop    path_test.cpio Videos
abc      Documents  petla       x2
abcd.txt Downloads  Pictures    z1
abc.txt  echo       Public
asas.txt eeee.tx    s1

root@student-VirtualBox:/home/student# mkdir /var/www/html/secure
root@student-VirtualBox:/home/student# cd /var/www/html/secure
root@student-VirtualBox:/var/www/html/secure# nano index.html
-----
index.html
root@student-VirtualBox:/var/www/html/secure#
```

2.9. Załaduj moduł ssl serwera Apache.

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

```
root@student-VirtualBox: /var/www/html/secure
abc.txt echo Public
asas.txt eeee.tx s1
root@student-VirtualBox:/home/student# mkdir /var/www/html/secure
root@student-VirtualBox:/home/student# cd /var/www/html/secure
root@student-VirtualBox:/var/www/html/secure# nano index.html
root@student-VirtualBox:/var/www/html/secure# ls
index.html
root@student-VirtualBox:/var/www/html/secure# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
root@student-VirtualBox:/var/www/html/secure# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
root@student-VirtualBox:/var/www/html/secure#
```

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

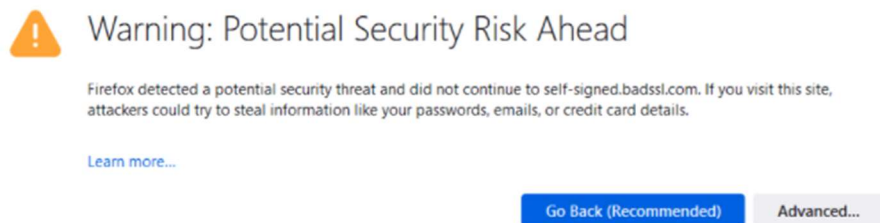


3. Wnioski

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 kłódkę 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.