Pytanie 1: Co to są protokoły szyfrowania wykorzystywane w transakcjach sieciowych?

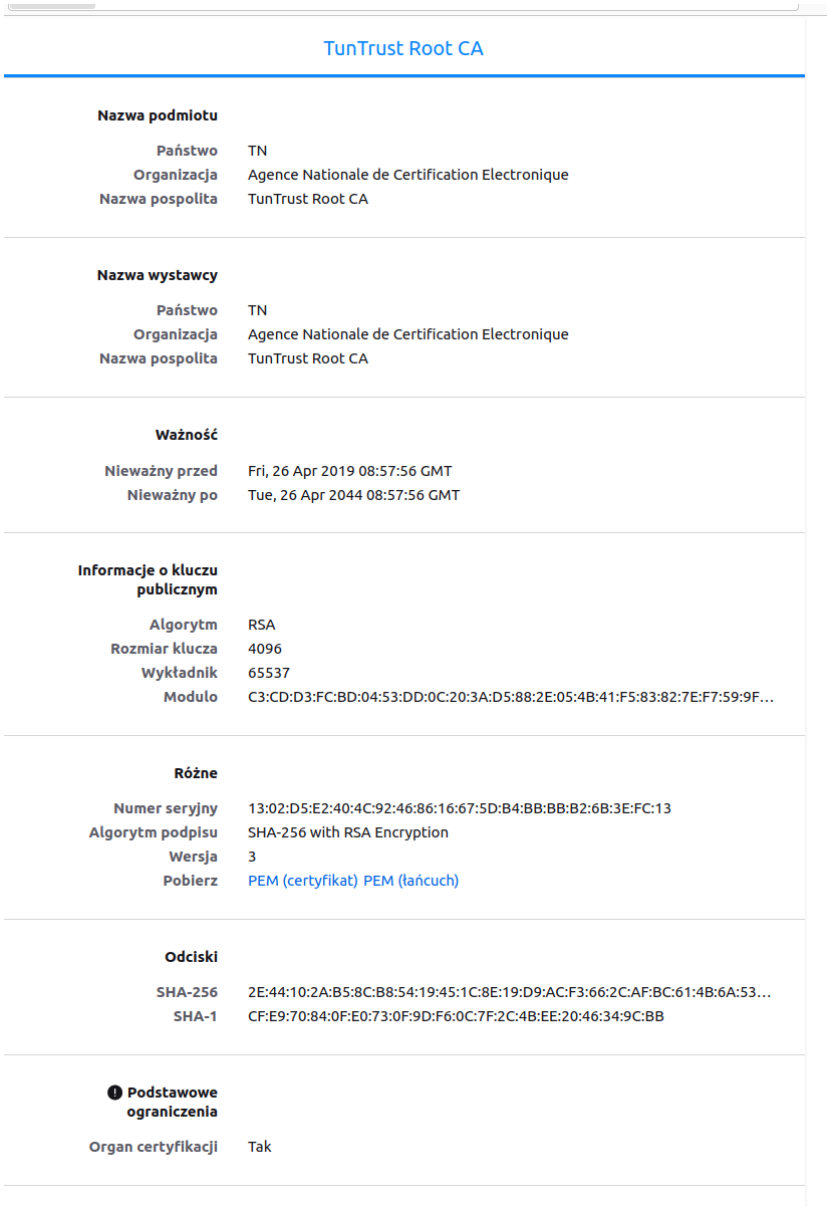
Protokoły szyfrowania wykorzystywane w transakcjach sieciowych to zestawy reguł i metod szyfrowania zapewniające bezpieczną wymianę danych między komputerami i serwerami w sieci.

Pytanie 2: Wymień dwie spośród tych nazw.

Chambers of Commerce Root – 2008

EC-ACC

Pytanie 3: Pobrać zrzut ekranu z certyfikatem i wkleić go do listy odpowiedzi.



TunTrust Root CA

**Nazwa podmiotu**

| | |
|---|---|
| Państwo | TN |
| Organizacja | Agence Nationale de Certification Electronique |
| Nazwa pospolita | TunTrust Root CA |

**Nazwa wystawcy**

| | |
|---|---|
| Państwo | TN |
| Organizacja | Agence Nationale de Certification Electronique |
| Nazwa pospolita | TunTrust Root CA |

**Ważność**

| | |
|---|---|
| Nieważny przed | Fri, 26 Apr 2019 08:57:56 GMT |
| Nieważny po | Tue, 26 Apr 2044 08:57:56 GMT |

**Informacje o kluczu publicznym**

| | |
|---|---|
| Algorytm | RSA |
| Rozmiar klucza | 4096 |
| Wykładnik | 65537 |
| Modulo | C3:CD:D3:FC:BD:04:53:DD:0C:20:3A:D5:88:2E:05:4B:41:F5:83:82:7E:F7:59:9F… |

**Różne**

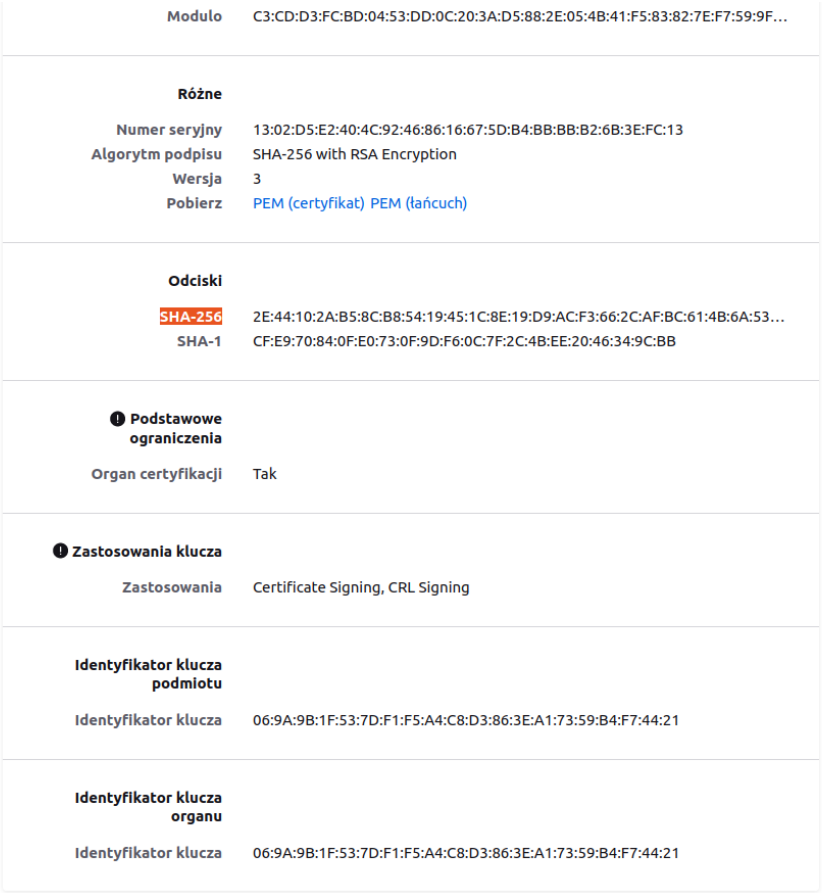
| | |
|---|---|
| Numer seryjny | 13:02:D5:E2:40:4C:92:46:86:16:67:5D:B4:BB:BB:B2:6B:3E:FC:13 |
| Algorytm podpisu | SHA-256 with RSA Encryption |
| Wersja | 3 |
| Pobierz | PEM (certyfikat) PEM (łańcuch) |

**Odciski**

| | |
|---|---|
| SHA-256 | 2E:44:10:2A:B5:8C:B8:54:19:45:1C:8E:19:D9:AC:F3:66:2C:AF:BC:61:4B:6A:53… |
| SHA-1 | CF:E9:70:84:0F:E0:73:0F:9D:F6:0C:7F:2C:4B:EE:20:46:34:9C:BB |

**Podstawowe ograniczenia**

| | |
|---|---|
| Organ certyfikacji | Tak |




Pytanie 4: Jaki algorytm wykorzystano w tym przypadku?

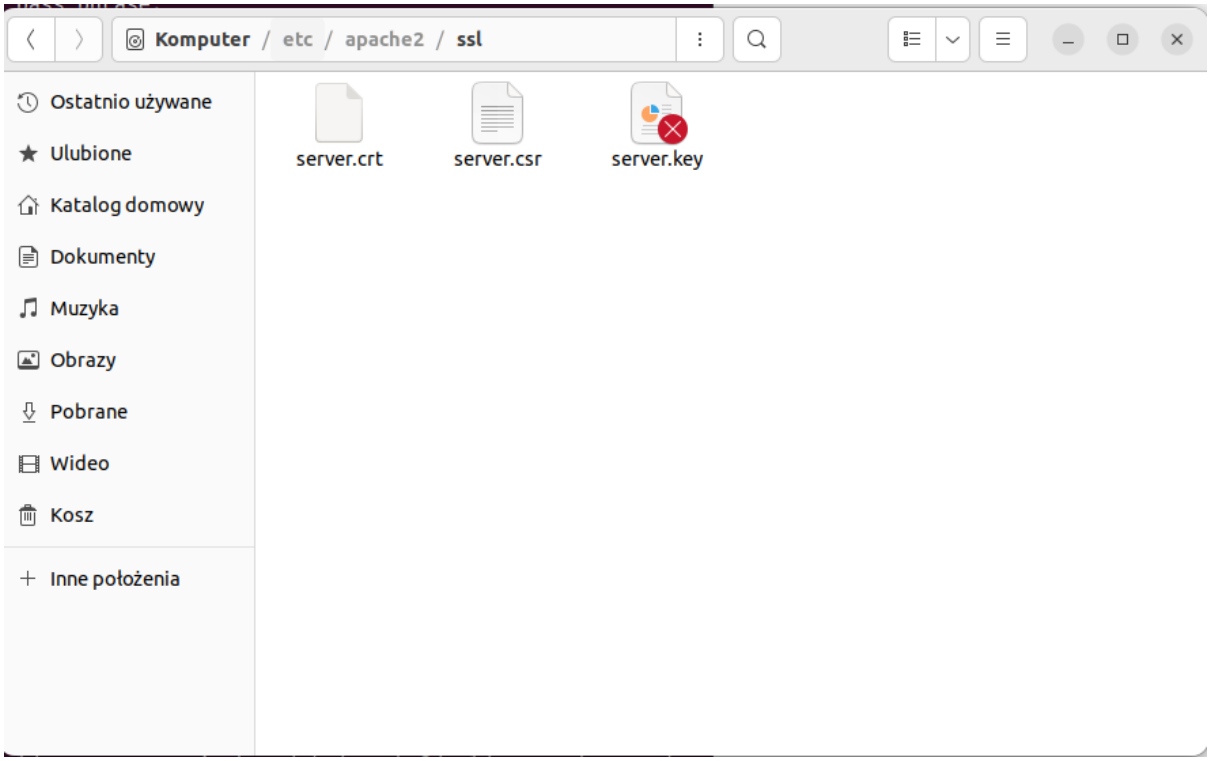
SHA-256

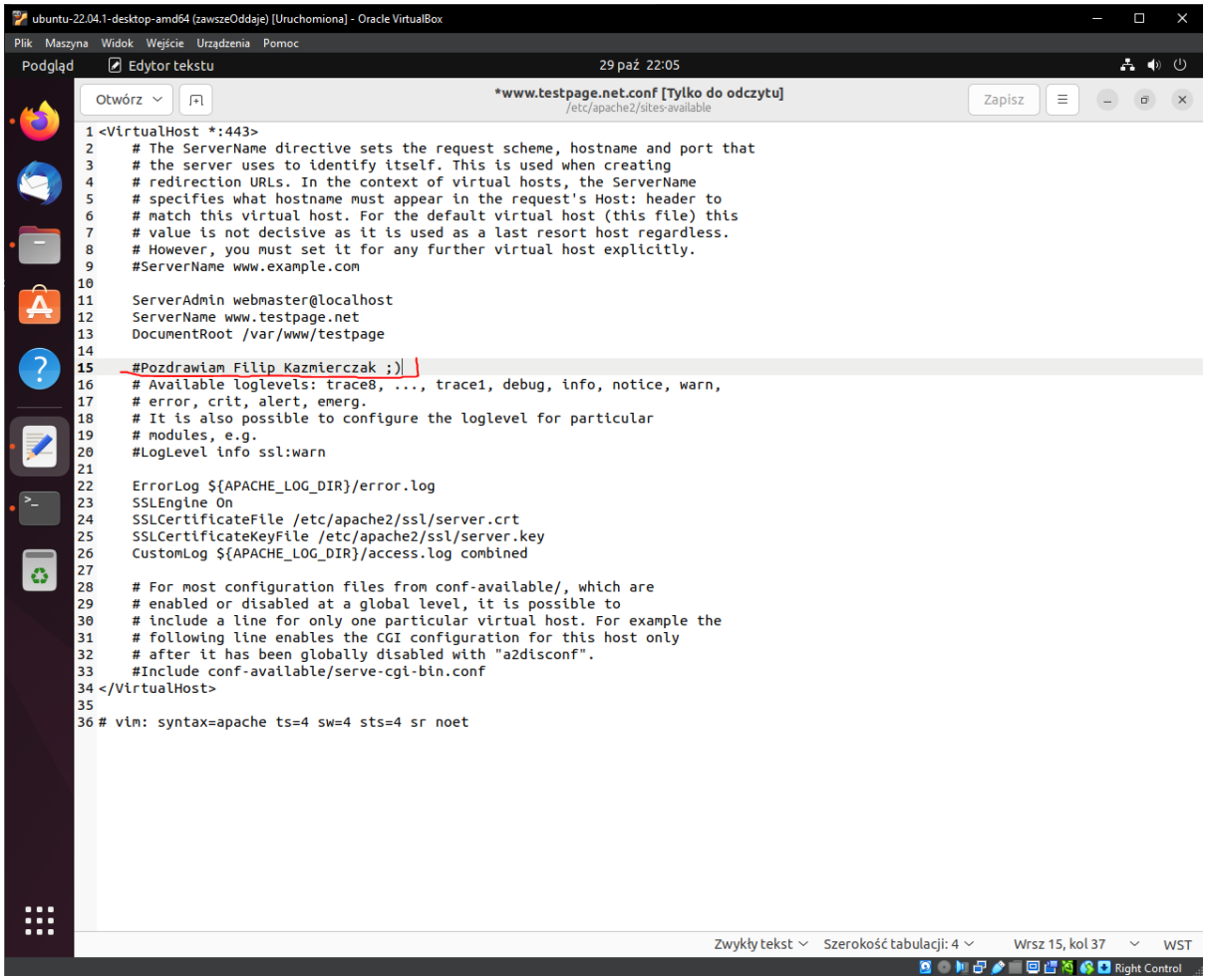
Pytanie 5: Jaka jest długość tego klucza w bitach?

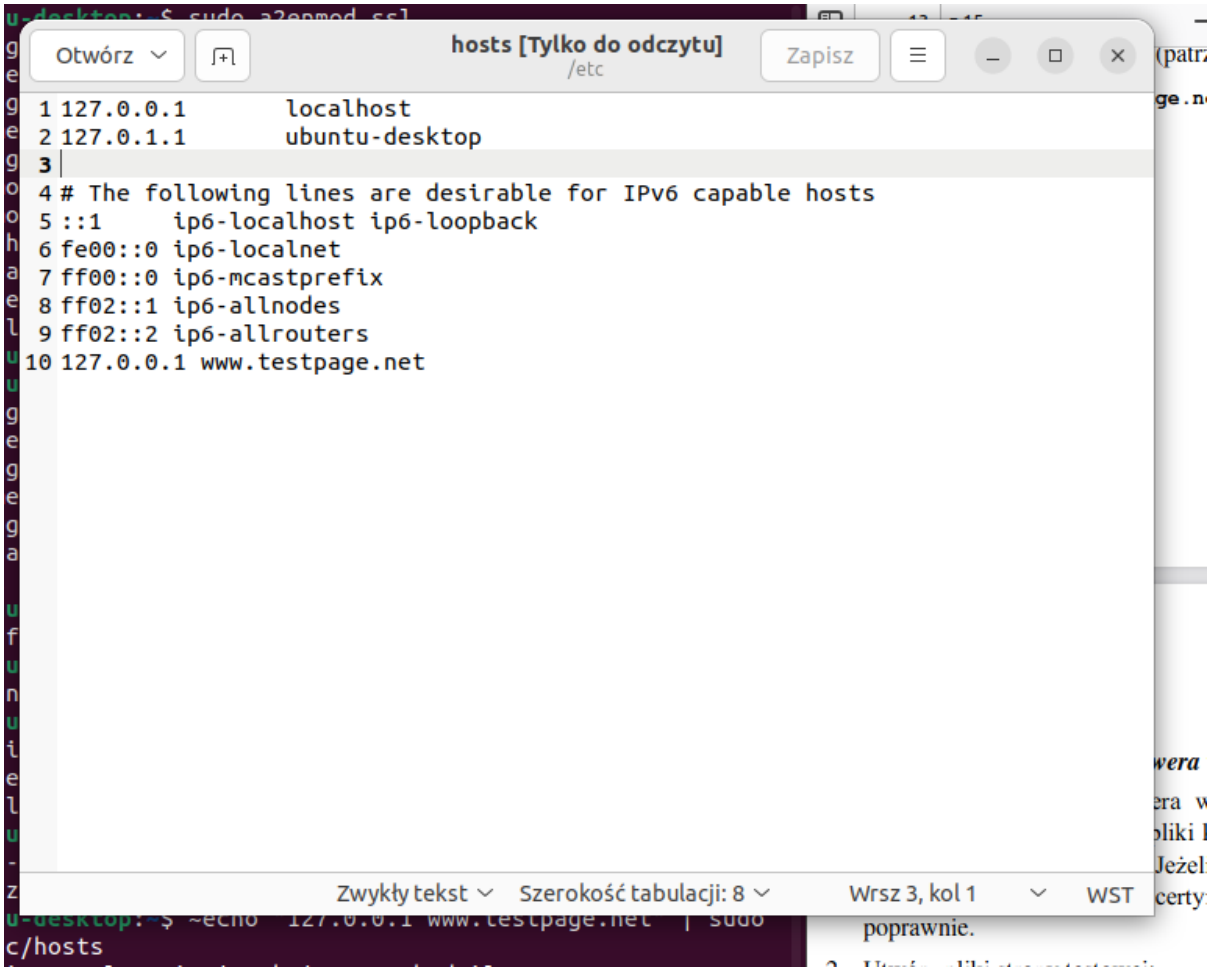
256

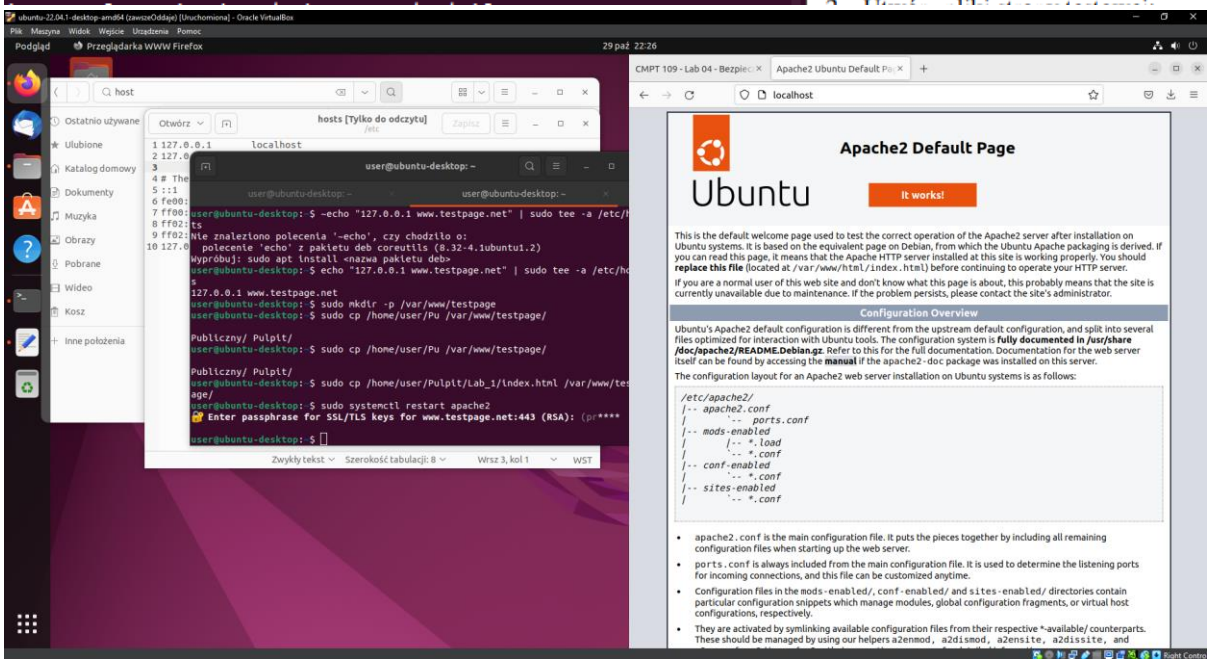
Pytanie 6: Z jakich powodów certyfikat może być nieważny?

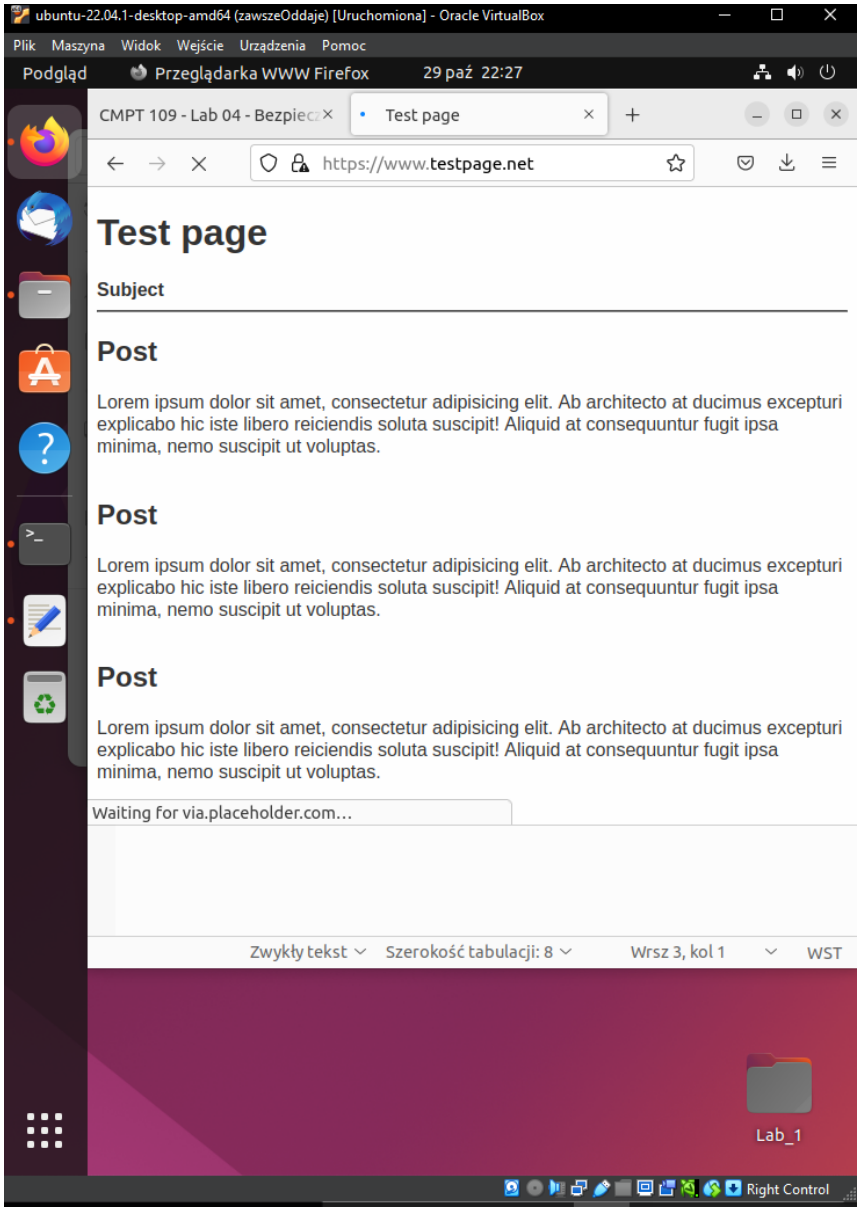
Upłynęła data ważności certyfikatu.


Komputer / etc / apache2 / ssl
Ostatnio używane
Ulubione
Katalog domowy
Dokumenty
Muzyka
Obrazy
Pobrane
Wideo
Kosz
Inne położenia
server.crt
server.csr
server.key


ubuntu-22.04.1-desktop-amd64 (zawszeOddaje) [Uruchomiona] - Oracle VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd
Edytor tekstu
29 paź 22:05
Otwórz
*www.testpage.net.conf [Tylko do odczytu]
/etc/apache2/sites-available
Zapisz
1 <VirtualHost *:443>
2 # The ServerName directive sets the request scheme, hostname and port that
3 # the server uses to identify itself. This is used when creating
4 # redirection URLs. In the context of virtual hosts, the ServerName
5 # specifies what hostname must appear in the request's Host: header to
6 # match this virtual host. For the default virtual host (this file) this
7 # value is not decisive as it is used as a last resort host regardless.
8 # However, you must set it for any further virtual host explicitly.
9 #ServerName www.example.com
10
11 ServerAdmin webmaster@localhost
12 ServerName www.testpage.net
13 DocumentRoot /var/www/testpage
14
15 #Pozdrawiam Filip Kazmierczak ;)
16 # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
17 # error, crit, alert, emerg.
18 # It is also possible to configure the loglevel for particular
19 # modules, e.g.
20 #LogLevel info ssl:warn
21
22 ErrorLog ${APACHE_LOG_DIR}/error.log
23 SSLEngine On
24 SSLCertificateFile /etc/apache2/ssl/server.crt
25 SSLCertificateKeyFile /etc/apache2/ssl/server.key
26 CustomLog ${APACHE_LOG_DIR}/access.log combined
27
28 # For most configuration files from conf-available/, which are
29 # enabled or disabled at a global level, it is possible to
30 # include a line for only one particular virtual host. For example the
31 # following line enables the CGI configuration for this host only
32 # after it has been globally disabled with "a2disconf".
33 #Include conf-available/serve-cgi-bin.conf
34 </VirtualHost>
35
36 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
Zwykły tekst
Szerokość tabulacji: 4
Wrsz 15, kol 37
WST
Right Control


Otwórz
hosts [Tylko do odczytu]
/etc
Zapisz
1 127.0.0.1 localhost
2 127.0.1.1 ubuntu-desktop
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 ip6-localhost ip6-loopback
6 fe00::0 ip6-localnet
7 ff00::0 ip6-mcastprefix
8 ff02::1 ip6-allnodes
9 ff02::2 ip6-allrouters
10 127.0.0.1 www.testpage.net
Zwykły tekst
Szerokość tabulacji: 8
Wrsz 3, kol 1
WST


Apache2 Default Page
Ubuntu
It works!
Configuration Overview



Test page

Subject

Post

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Ab architecto at ducimus excepturi explicabo hic iste libero reiciendis soluta suscipit! Aliquid at consequuntur fugit ipsa minima, nemo suscipit ut voluptas.

Post

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Ab architecto at ducimus excepturi explicabo hic iste libero reiciendis soluta suscipit! Aliquid at consequuntur fugit ipsa minima, nemo suscipit ut voluptas.

Post

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Ab architecto at ducimus excepturi explicabo hic iste libero reiciendis soluta suscipit! Aliquid at consequuntur fugit ipsa minima, nemo suscipit ut voluptas.

Pytanie 7: Jaki jest okres ważności tego certyfikatu?

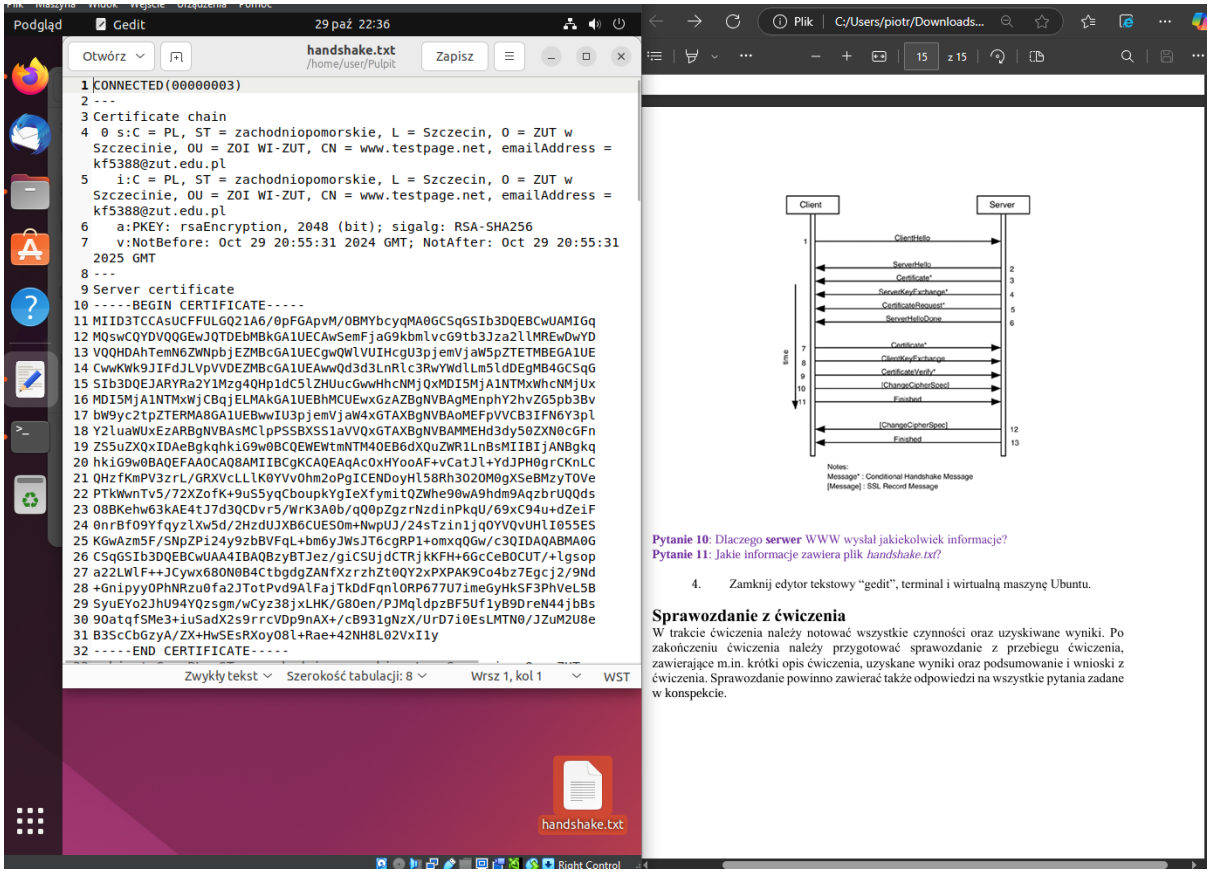
365 dni

Pytanie 8: Kto jest wystawcą tego certyfikatu?

Wystawcą certyfikatu jest serwer, który samodzielnie podpisuje swój certyfikat.

Pytanie 9: Jaka jest funkcja certyfikatu podczas komunikacji sieciowej między przeglądarką i Twoim serwerem WWW?

Certyfikat służy do uwierzytelniania serwera WWW, zapewniając klientowi, że połączenie jest zaufane




Pytanie 10: Dlaczego serwer WWW wysłał jakiekolwiek informacje?

Serwer WWW wysyła informacje, aby odpowiedzieć na żądanie klienta, który chce ustanowić bezpieczne połączenie.

Pytanie 11: Jakie informacje zawiera plik handshake.txt?

Zawiera szczegóły związane z procesem negocjacji SSL, w tym informacje na temat certyfikatu serwera i parametrów szyfrowania.