PROJECT 12
Server https

Kebutuhan Projek:

- Sebuah komputer Linux machine, real atau virtual. Bisa menggunakan BackTrack 5 virtual machine.

Menjalankan Komputer Linux

1. Jalankan komputer seperti biasa. Buka jendela Terminal.
2. Pada jendela Terminal, masukan perintah berikut, dan tekan Enter:

   `ping www.binadarma.ac.id`

   Pastikan ada balasan replies. Jika tidak, maka perlu memperbaiki masalah jaringan.

Menggenerate Server Key

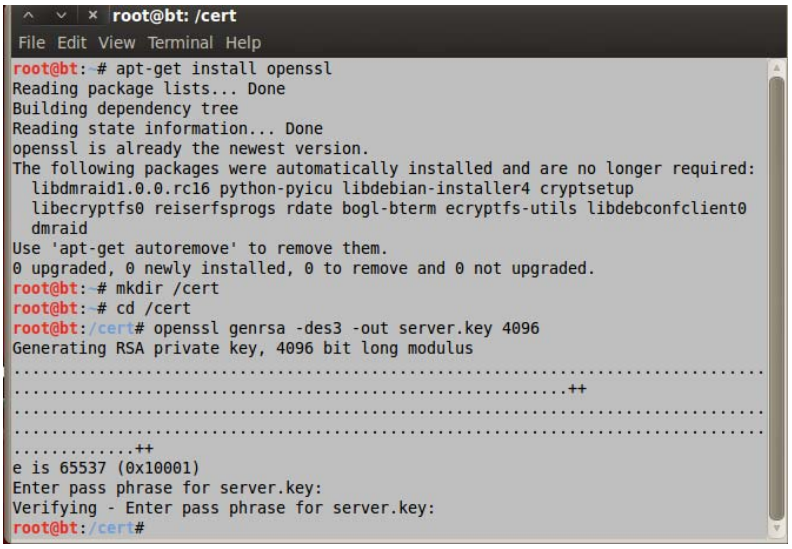
3. Pada jendela Terminal, masukan perintah berikut, akhiri dengan Enter masing-masing baris:

`apt-get remove --purge openssl` *(untuk uninstall openssl dan sertifikat yang sdh terinstal sebelumnya)*

```
apt-get install openssl
mkdir /cert
cd /cert
openssl genrsa -des3 -out server.key 4096
```

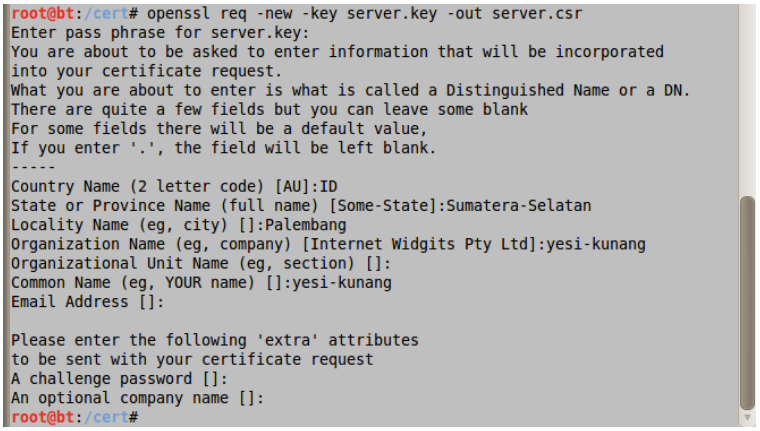
4. Ketika muncul pesan: "Enter pass phrase for server.key:" ketikan passphrase.

   *Untuk project ini disarankan menggunakan frase **password** – gunakan yang lebih password yang lebih aman untuk server real.*
   Ketika diminta memasukan passphrase yang kedua kali, masukan. Tidak akan terlihat apa-apa di layar pada saat saudara mengetikan passphrases, ini normal di Linux.



Membuat Certificate Request

5. Pada jendela Terminal window, masukan perintah berikut, dan tekan:
   `openssl req -new -key server.key -out server.csr`
   Masukkan passphrase : **password**
   Masukkan Country Name : **ID**
   Masukkan State or Province Name : **Sumatera-Selatan**
   Masukkan Locality Name : **Palembang**
   Masukkan Organization Name : **YOUR NAME** – jangan masukan "YOUR NAME" – gunakan nama sendiri.
   Masukkan Orgizational Unit Name kosong, dengan menekan **Enter**.
   Masukkan Common Name : **YOUR NAME** – jangan masukkan "YOUR NAME" – gunakan nama sendiri.
   Email Address biarkan kososng, dengan menekan **Enter**.
   Challenge Password biarkan kosong, dengan menekan **Enter**.
   "optional company name" biarkan kosong, dengan menekan **Enter**.



Sign Certificate Signing Request

6. Pada jendela Terminal, masukan perintah berikut, dan tekan Enter:

`openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt`

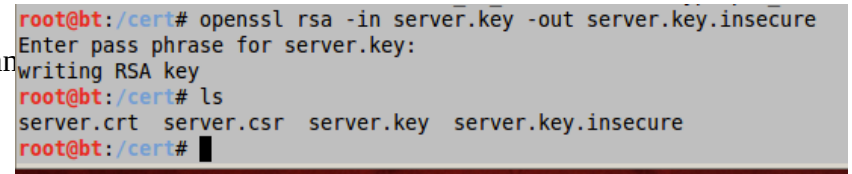
Ketika meminta passphrase, ketikan **password**

Membuat Server Key yang tidak Membutuhkan Password

7. Pada jendela Terminal, masukkan perintah berikut, dengan menekan Enter setiap baris. Ketika muncul passphrase, ketikkan **password**
   `openssl rsa -in server.key -out server.key.insecure`
   `mv server.key server.key.secure`
   `mv server.key.insecure server.key`

Empat File yang dihasilkan

8. Pada jendela Terminal, masukkan perintah berikut, dan tekan Enter:
   `ls`

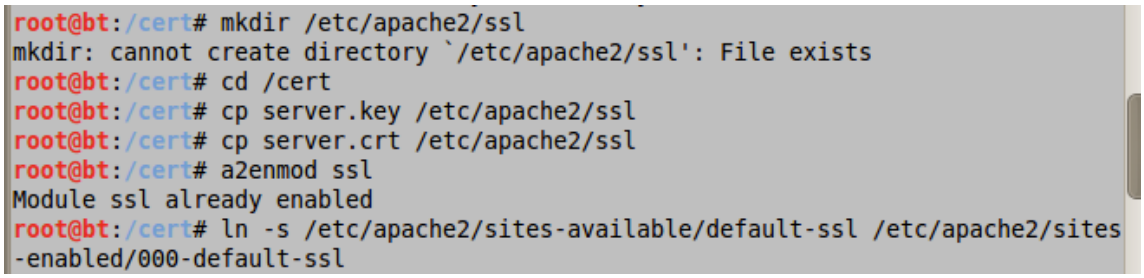


Catatan karakter pertama adalah L huruf kecil, bukan angka 1.
Akan terdapat empat file berikut:
server.crt: self-signed server certificate (sertifikat server).
server.csr: Server certificate signing request (sertifikat untuk menandai permintaan).
server.key: The private server key, does not require a password when starting Apache.
server.key.secure: The private server key, it does require a password when starting Apache.

Konfigurasi Apache untuk SSL

9. Pada jendela Terminal, masukkan perintah berikut, tekan Enter setelah selesai. Ketika muncul passphrase, masukan **password**

```
mkdir /etc/apache2/ssl
cd /cert
cp server.key /etc/apache2/ssl
cp server.crt /etc/apache2/ssl
a2enmod ssl
ln -s /etc/apache2/sites-available/default-ssl
/etc/apache2/sites-enabled/000-default-ssl
```



Membuat Secure Document Root

10. Perintah berikut membuat direktori /var/www-ssl, yang merupakan direktori untuk halaman web yang secure. In a Pada jendela Terminal, masukan perintah berikut, tekan Enter setiap baris.

```
cd /var
mkdir www-ssl
```

Memback Up Konfigurasi File Apache

11. Pada jendela Terminal, masukkan perintah berikut, tekan Enter tiap baris.

```
cd /etc/apache2/sites-available
cp /etc/apache2/sites-available/default
default_original
cp /etc/apache2/sites-available/default-ssl default-
ssl_original
```

Konfigurasi Virtual Hosts

12. Pada jendela Terminal, masukan perintah berikut, dan kemudian tekan Enter:
    `ifconfig`

    Lihat Alamat IP dan catat.
    Catatan: Jika alamat IP berubah, perlu mengedit dua file di instruksi 14 dan 15 .

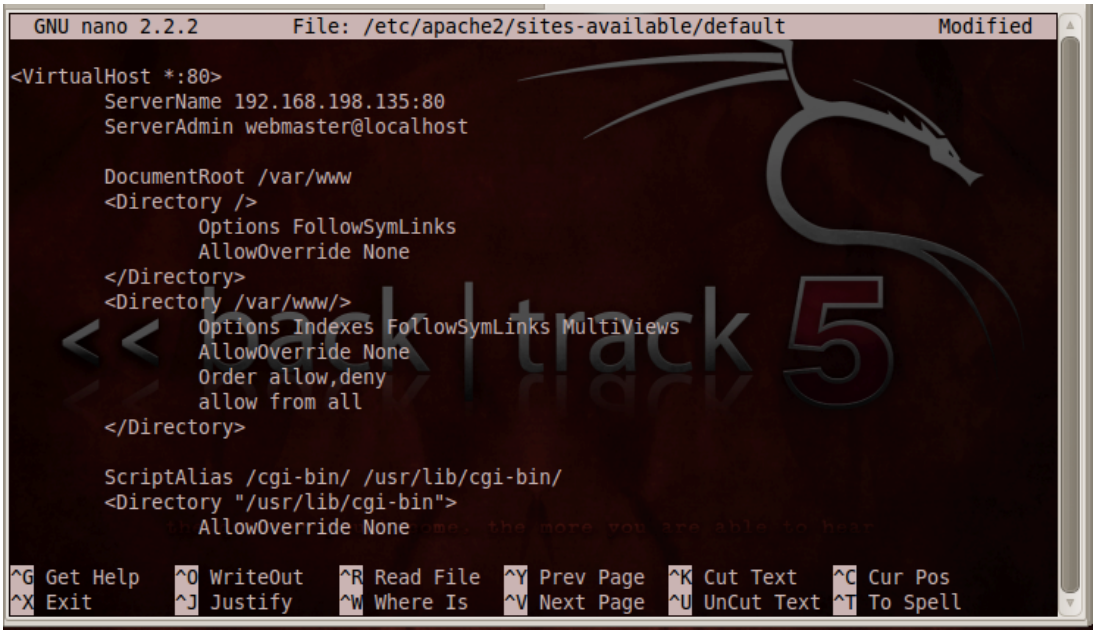
13. Pada jendela Terminal, masukkan perintah berikut, dan tekan Enter:

    `nano /etc/apache2/sites-available/default`

14. Pada text editor, tambahkan baris berikut **<VirtualHost *:80>**, gunakan alamat IP yang didapat pada point 12 seperti contoh berikut:

    `ServerName 192.168.77.xx:80`

    Maka akan dapat seperti pada gambar:



15. Tkan **Ctrl+X**, **Y**, **Enter** untuk menyimpan file. Pada jendela Terminal, masukkan perintah berikut, kemudian tekan Enter:

    `nano /etc/apache2/sites-available/default-ssl`

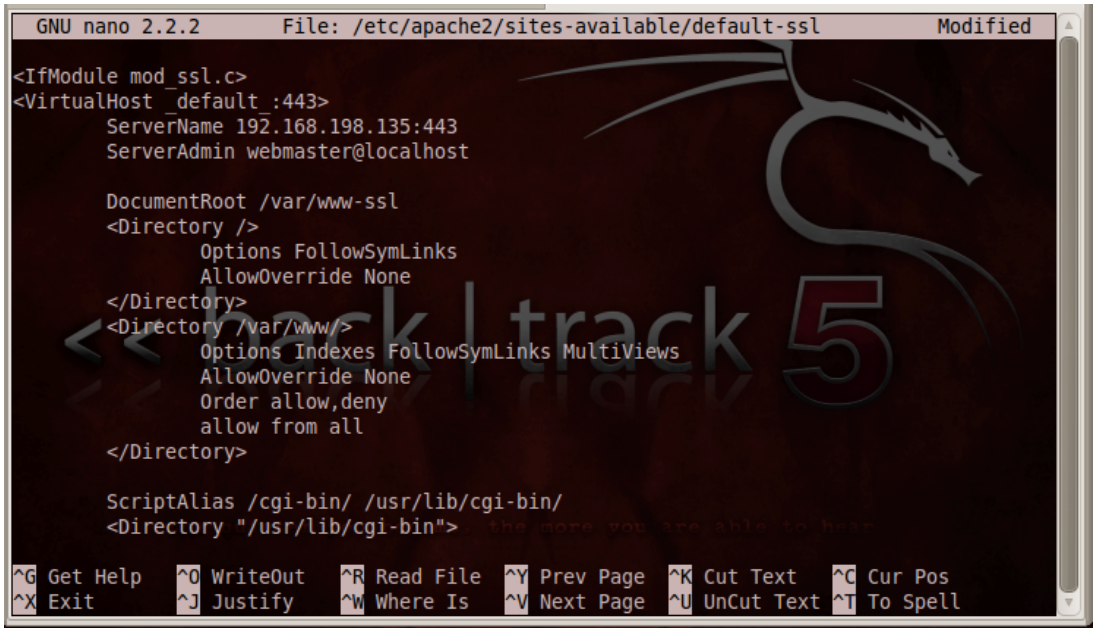
16. Pada jendela text editor, tambahkan baris berikut setelah baris **<VirtualHost *:443>**, gunakan alamat IP di langkah 12:

    `ServerName 192.168.77.XX:443`

    Rubah baris berikut:

    `DocumentRoot /var/www`
    menjadi
    `DocumentRoot /var/www-ssl`

    File harus seperti Nampak pada gambar:



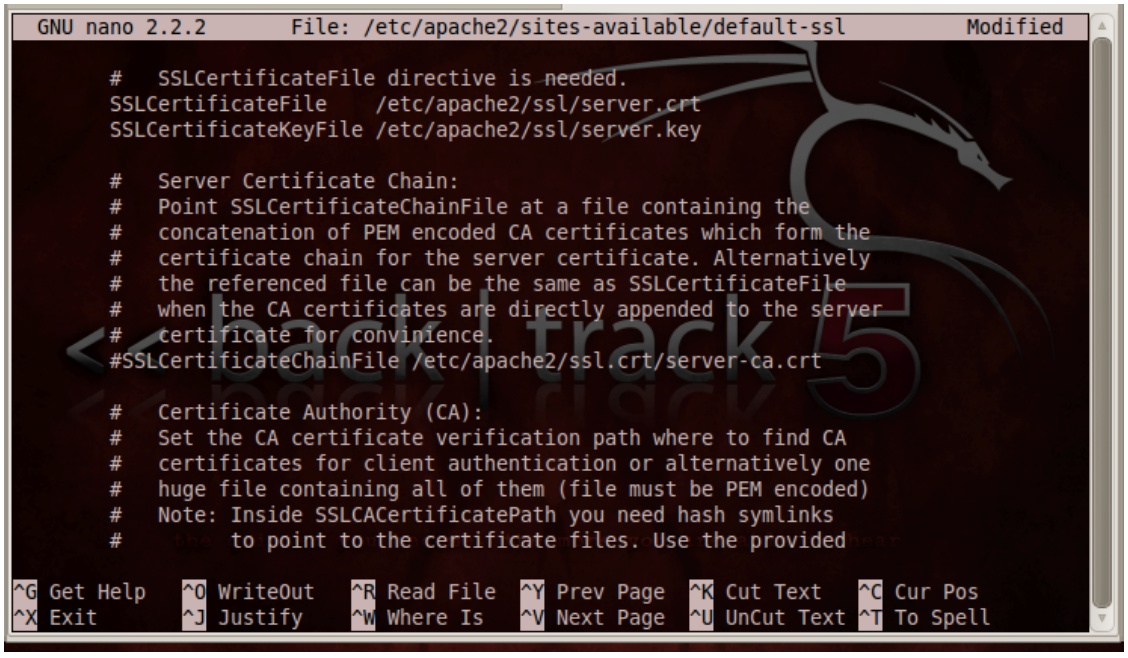
Scroll down dan cari dua baris berikut (bisa jadi sudah dirubah sebelumnya)

```
SSLCertificateFile /etc/ssl/certs/ssl-cert-
snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-
snakeoil.key
```

Rubah menjadi seperti ini:

```
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
```

File harus menjadi seperti pada gambar berikut:



Tekan **Ctrl+X**, **Y**, **Enter** simpan file.

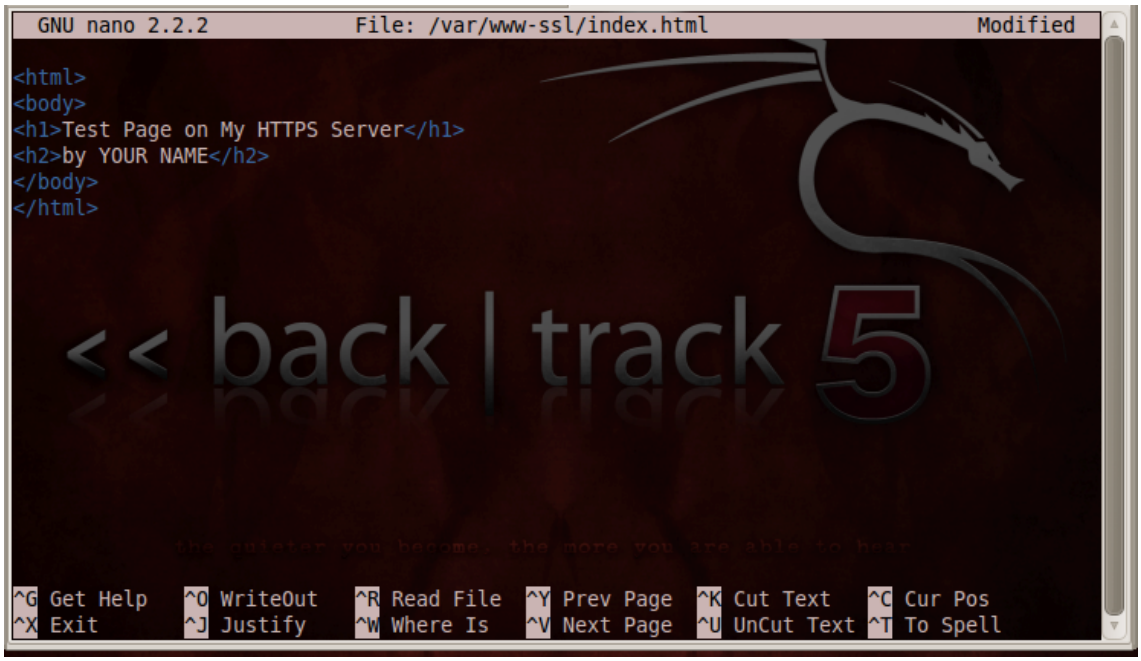
Membuat halaman Web Demonstrasi

17. Pada jendela Terminal, masukkan perintah berikut dan tekan Enter:
    `nano /var/www-ssl/index.html`

    Pada text editor, masukkan code berikut, ganti "YOUR NAME" dengan nama sendiri:

```
<html>
<body>
<h1>Test Page on My HTTPS Server</h1>
<h2>by YOUR NAME</h2>
</body>
</html>
```

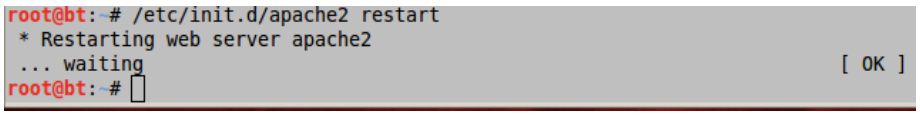
    File akan Nampak seperti berikut:



    Tekan **Ctrl+X**, **Y**, **Enter** untuk menyimpan file.

Restart Apache

18. Pada jendela Terminal, masukan perintah berikut, dan tekan Enter:



    `/etc/init.d/apache2 restart`

Melihat Halaman Secure Web Page

19. Dari jendela Linux desktop sebelah kiri atas, click **Applications**, **Internet**, **Firefox Web Browser**.
20. Masukan URL berikut, dan tekan Enter:

    https://localhost

21. Akan muncul pesan "This Connection is Untrusted". Hal ini dikarenakan sertifikat SSL kita buat sendiri (self-signed), bukan dari CA (Certificate Authority) resmi seperti Verisign.
22. Click "**I Understand the Risks**".
23. Click tombol "**Add Exception**".
24. Click tombol "**Confirm Security Exception**" .
25. Halaman secure web page akan terbuka, seperti berikut:

Simpan Screen Image

26. Pastikan URL dimulai dengan **https:**, dan nama yang muncul memperlihatkan nama kalian seperti di atas.
27. Simpan screen capture dengan nama file "**NamaKamu_Proj 12** ".
28. Kumpulkan project melalui elearning.

Sumber:

http://www.tc.umn.edu/~brams006/selfsign.html

Last Modified: 12-11-12