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 masingmasing 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

FCNS -- Yesi Novaria Kunang , S.T., M.Kom.

Project 12: server https

```
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.
                                                                        t# openssl req -new -key server.key -out server.csr
                                                          Enter pass phrase for server.key:
     Masukkan Orgizational Unit Name
                                                          You are about to be asked to enter information that will be incorporated 
into your certificate request.
     kosong, dengan menekan Enter.
                                                          What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
     Masukkan Common Name : YOUR
     NAME – jangan masukkan "YOUR
                                                          If you enter '.', the field will be left blank.
     NAME" – gunakan nama sendiri.
                                                          Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Sumatera-Selatan
     Email Address biarkan kososng,
                                                          Locality Name (eg, city) []:Palembang
Organization Name (eg, company) [Internet Widgits Pty Ltd]:yesi-kunang
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:yesi-kunang
Email Address []:
      dengan menekan Enter.
     Challenge Password biarkan kosong,
     dengan menekan Enter.
      "optional company name" biarkan
                                                          Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
     kosong, dengan menekan Enter.
                                                                bt:/
```

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
```

```
File Edit View Terminal Help
Foot@bt:/cert# openssl x509 -req -days 365 -in server.csr -signkey server.key -0 *
ut server.crt
Signature ok
subject=/C=ID/ST=Sumatera-Selatan/L=Palembang/0=yesi-kunang/CN=yesi-kunang
Getting Private key
Enter pass phrase for server.key:
root@bt:/cert# []
```

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

Pada jendela Terminal, masukkan perintah berikut, dan tekan Enter:
 1s

FCNS -- Yesi Novaria Kunan writing RSA key root@bt:/cert# ls server.crt server.key server.key.insecure root@bt:/cert# 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

```
root@bt:/cert# mkdir /etc/apache2/ssl
mkdir: cannot create directory `/etc/apache2/ssl': File exists
root@bt:/cert# cd /cert
root@bt:/cert# cp server.key /etc/apache2/ssl
root@bt:/cert# cp server.crt /etc/apache2/ssl
root@bt:/cert# a2enmod ssl
Module ssl already enabled
root@bt:/cert# ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites
-enabled/000-default-ssl
```

Membuat Secure Document Root

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
```

```
root@bt:/cert# cd /var
root@bt:/var# mkdir www-ssl
root@bt:/var# cd /etc/apache2/sites-available
root@bt:/etc/apache2/sites-available# cp /etc/apache2/sites-available/default de
fault_original
root@bt:/etc/apache2/sites-available# cp /etc/apache2/sites-available/default-ss
l default-ssl_original
root@bt:/etc/apache2/sites-available# ifconfig
```

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:

GNU nano 2.	2.2 Fil	.e: /etc/apache	2/sites-availa	able/default	Modified
<virtualhost Serve Serve</virtualhost 	*:80> erName 192.168 erAdmin webmast	198.135:80 cer@localhost			
Docum <dire <td>nentRoot /var/w cctory /> Options Fol AllowOverri rectory> ectory /var/www Options Ind AllowOverri Order allow allow from rectory></td><td>₩₩ lowSymLinks de None //> lexes FollowSym de None /,deny all</td><td>⊨inks MultiVie</td><td>wsk 55</td><td></td></dire 	nentRoot /var/w cctory /> Options Fol AllowOverri rectory> ectory /var/www Options Ind AllowOverri Order allow allow from rectory>	₩₩ lowSymLinks de None //> lexes FollowSym de None /,deny all	⊨inks MultiVie	wsk 55	
Scrip <dire< td=""><td>otAlias /cgi-bi ectory "/usr/li AllowOverri</td><td>in/ /usr/lib/cg b/cgi-bin"> de None</td><td>ji-bin/</td><td></td><td></td></dire<>	otAlias /cgi-bi ectory "/usr/li AllowOverri	in/ /usr/lib/cg b/cgi-bin"> de None	ji-bin/		
<mark>^G</mark> Get Help <mark>^X</mark> Exit	<mark>^0</mark> WriteOut <mark>^J</mark> Justify	^R Read File ^₩ Where Is	<pre>^Y Prev Page ^V Next Page</pre>	<pre>^K Cut Text ↑C Cur ^U UnCut Text ↑T To</pre>	Pos Spell

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:

Project 12: server https

GNU nano 2.2.2 File: /etc/apache2/sites-available/default-ssl Modified					
<ifmodule mod_ssl.c=""> <virtualhost _default_:443=""> ServerName 192.168.198.135:443 ServerAdmin webmaster@localhost</virtualhost></ifmodule>					
DocumentRoot /var/www-ssl <directory></directory> Options FollowSymLinks AllowOverride None Options Indexes FollowSymLinks MultiViews AllowOverride None Order allow,deny allow from all 					
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/ <directory "="" cgi-bin"="" lib="" usr=""> the more you are able to how</directory>					
<pre>^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos ^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell ▼</pre>					

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:

GNU nano 2.2.2 File: /etc/apache2/sites-available/default-ssl Modified				
<pre># SSLCertificateFile directive is_needed. SSLCertificateFile /etc/apache2/ssl/server.crt SSLCertificateKeyFile /etc/apache2/ssl/server.key</pre>				
<pre># Server Certificate Chain: # Point SSLCertificateChainFile at a file containing the # concatenation of PEM encoded CA certificates which form the # certificate chain for the server certificate. Alternatively # the referenced file can be the same as SSLCertificateFile # when the CA certificates are directly appended to the server # certificate for convinience. #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt</pre>				
<pre># Certificate Authority (CA): # Set the CA certificate verification path where to find CA # certificates for client authentication or alternatively one # huge file containing all of them (file must be PEM encoded) # Note: Inside SSLCACertificatePath you need hash symlinks # to point to the certificate files. Use the provided</pre>				
<pre>^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos ^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell</pre>				

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

<pre>root@bt: # /etc/init.d/apache2 restart * Restarting web server apache2 waiting root@bt: # </pre>	[ОК]
ekan Enter:	
	<pre>root@bt:~# /etc/init.d/apache2 restart * Restarting web server apache2 waiting root@bt:~# ekan Enter:</pre>

/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