04_LINUX_SSL

작 성 일 : 20.01.07.

작 성 자 : 김 한 석

- **SSL(Secure Sockets Layer)**
  - 웹 서버 인증, 서버 인증이라고 불리는, 클라이언트와 서버의 **통신을 제 3자가 보증해주는 전자화된 문서**
  - **이점**
    - 통신 내용이 공격자에게 **노출되는 것을 막을 수 있다**.
    - 클라이언트가 접속하려는 서버가 **신뢰할 수 있는 서버인지를 판단**할 수 있다.
    - 통신 내용의 **악의적인 변경을 방지**할 수 있다.
- **SSL과 HTTPS는 같은 것일까?**
  - HTTPS는 SSL 프로토콜 위에서 돌아가는 프로토콜
  - HTTPS로 데이터 전송을 시작할 때, SSL이 데이터 보안을 제공

1. Ubuntu

1.1 OpenSSL 설치 및 인증서 생성

- apt-get 패키지 업데이트

```
$ sudo apt-get update
```

- OpenSSL 설치 확인

```
$ sudo openssl version
```

- OpenSSL 설치

```
$ sudo apt-get install openssl
```

1.1.1 개인키 생성

- 개인키 생성

```
$ sudo openssl genrsa -des3 -out server.key 2048

Generating RSA private key, 2048 bit long modulus
..+++
.................+++
e is 65537(0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key
```

- `Enter pass phrase for server.key` : 임의의 개인키 암호를 입력

1.1.2 인증요청서(Certificate Sinning Request, CSR) 생성

- CSR 생성

```
$ sudo openssl req -new -days 365 -key server.key -out server.csr # 365는 유효기간 생략可
Enter pass phrase for server.key:   # 위에서 만든 개인키를 입력
```

- 각종 정보 입력

```
Country Name (2 letter code) [AU] : KR
State or Province Name (full name) [Some-State] : Seoul
Locality Name (eg, city) [] :
Organization Name (eg, company) [Internet Widgits Pty Ltd] :
Organizational Unit Name (eg, section) [] :
Common Name (e.g. server FQDN or YOUR name) [] :
Email Address [] :
```

- 추가 정보 입력(Enter 두번으로 그냥 넘어가자)

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password [] :
An optional company name [] :
```

1.1.3 개인키 패스워드 제거

> - 개인키에 패스워드가 있으면 아파치 구동 시마다 물어본다.
> - 편의를 위해 개인키 패스워드를 제거한다. 패스워드를 제거하더라도 SSL에는 문제가 없다.

- 기존 개인키 복사

```
$ sudo cp server.key server.keyorigin
```

- 개인키 패스워드 제거

```
$ sudo openssl rsa -in server.key.origin -out server.key
Enter pass phrase for server.key.origin:    # 개인키 입력
```

1.1.4 인증서 생성

- 개인키와 인증 요청서를 가지고 인증서를 생성

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

- 성공 시

```
Signature ok
subject=/C=KR/ST=Seoul/L={ local }/O={ company }/OU={ section }/CN={ name }/emailAddress={ email }
Getting Private key
```

1.1.5 인증서 확인

- 인증서 확인

```
$ ls -l server*
```

- 개인키 확인

```
$ cat server.key | head -3
-----BEGIN RSA PRIVATGE KEY-----
```

- 인증서 확인

```
$ cat server.crt | head -3
-----BEGIN CERTIFICATE-----
```

1.2 Apache에 SSL 적용

1.2.1 SSL 디렉토리 생성 및 인증서 복사

- 관리의 편의를 위해 ssl 인증서를 모아둘 디렉토리를 생성

```
$ sudo mkdir /etc/apache2/ssl
```

- 생성된 디렉토리로 인증서를 복사

```
$ sudo cp server.crt /etc/apache2/ssl/server.crt
$ sudo cp server.csr /etc/apache2/ssl/server.csr
$ sudo cp server.key /etc/apache2/ssl/server.key
```

- 복사 확인

```
$ cd /etc/apache2/ssl/
$ ls
server.crt  server.csr  server.key
```

1.2.2 SSL 모듈 활성

```
$ sudo a2enmod ssl
```

1.2.3 /etc/apache2/ports.conf 파일 수정

```
$ sudo vi /etc/apache2/ports.conf

# 내용 추가
<IfModule mod_ssl.c>
    LISTEN 443
</IfModule>
```

1.2.4 default-ssl.conf 파일 복사

- default-ssl.conf 파일을 복사해서 board-ssl.conf로 이름을 변경하였따.
- 복사한 파일명은 본인이 알기 쉽게 정하면 된다.

```
$ sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/board-ssl.conf
```

1.2.5 복사한 파일 수정

- 위에서 복사한 파일을 수정

```
$ sudo vi /etc/apache2sites-available/board-ssl.conf

# 해당부분 확인
SSLEngine on

# 해당부분 수정
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

# #을 제거
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
```

1.2.6 board-ssl 활성화

```
$ sudo a2ensite board-ssl
```

1.2.7 방화벽 설정

- 방화벽에 OpenSSL의 포트인 443 포트로 접속을 허용하도록 변경

```
$ sudo ufw allow 443/tcp
```

- 설정 후 443 포트 확인

```
$ netstat -anp | grep LISTEN | grep 443
```

- 정상적으로 동작 시

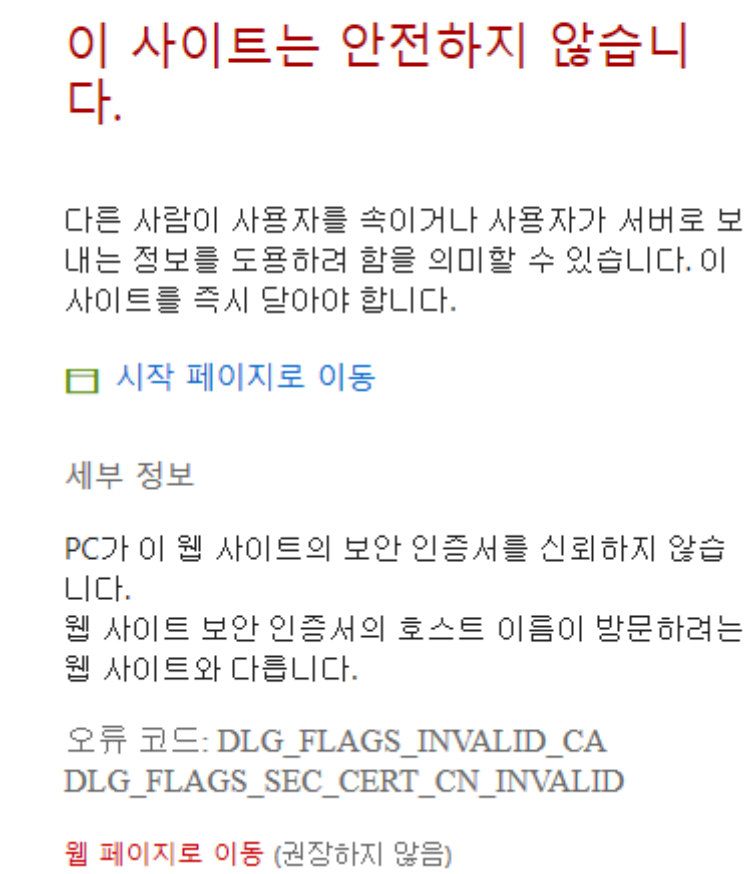
```
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp6       0      0 :::443                  :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      -
bizspring@ubuntu:/$ sudo /etc/init.d/apache2 restart
```

1.2.8 아파치 재시작

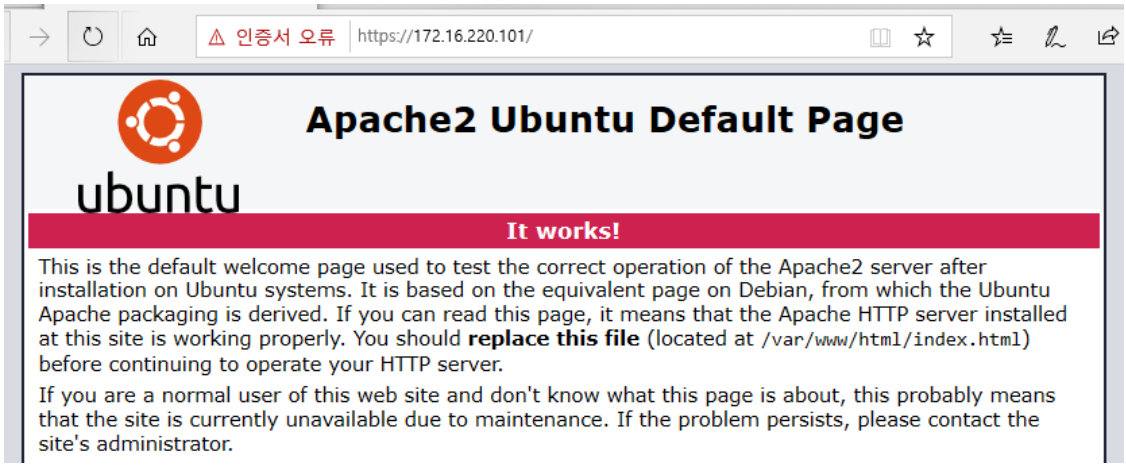
```
$ sudo /etc/init.d/apache2 restart
```

1.2.9 SSL 적용 확인

- `https://IP` 접속 시



- 웹 페이지로 이동 시



2. CentOS

2.1 OpenSSL 설치 및 인증서 생성

- CentOS 6 이상 버전은 기본적으로 OpenSSL 패키지가 설치되어 있다.
- 설치 확인

```
$ rpm -qa openssl
or
$ openssl version
```

2.1.1 개인키 생성

```
$ openssl genrsa -des3 -out server.key 2048
```

2.1.2 인증요청서(Certificate Sinning Request, CSR) 생성

```
$ openssl req -new -key server.key -out server.csr

# 개인키 입력
Enter pass phrase for server.key:
...

# 각종 정보입력
Country Name (2 letter code) [XX] : KR
State or Province Name (full name) [] :Seoul
Locality Name (eg, city) [Default City] :
Organizational Name (eg, company) [Default Company Ltd] :
Organizational Unit Name (eg, section) [] :
Common Name (eg, your name or your server's hostname) [] :
Email Address [] :
...

# 추가 정보 입력 Enter 2번을 넘어가자
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password [] :
An optional company name [] :
```

2.1.3 개인키 패스워드 제거

```
$ cp server.key server.key.origin
$ openssl rsa -in server.key.origin -out server.key
Enter pass phrase for server.key.origin:
```

2.1.4 인증서 생성

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

2.1.5 인증서 확인

```
$ cat server.key | head -3
$ cat server.crt | head -3
```

2.2 Apache에 SSL 적용

2.2.1 개인키와 인증서 설치

- 해당 디렉토리에 위치해야만 SSL 서비스를 제대로 제공해줄 수 있다.

```
$ cp server.crt /etc/pki/tls/certs
$ cp server.key /etc/pki/tls/private/server.key
$ cp server.csr /etc/pki/tls/private/server.csr
```

2.2.2 SSL 설정을 변경하기 위한 수정

- 수정 경로

```
$ sudo vi /etc/httpd/conf.d/ssl.conf
```

- 수정 사항
  - 수정 사항을 찾으려면 `ESC`를 누르고 `/` 입력 후 `검색어`를 입력후 `ENTER`, 다음 단어는 `n`을 눌러 이동
  - 수정 전

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

  - 수정 후

```
SSLCertificateFile /etc/pki/tls/certs/server.crt
SSLCertificateKeyFile /etc/pki/tls/private/server.key
```

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/server.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/server.key
```

2.2.3 서비스 적용을 위한 재시작

```
$ sudo service httpd restart
```

2.2.4 443 포트를 열기위해서 VirtualHost 추가

- 수정 경로

```
$ sudo vi /etc/httpd/conf/httpd.conf
```

- 을 열고 파일의 맨 아래에 다음 사항 추가

```
NameVirtualHost *:443
<VirtualHost *:443>
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/server.crt
    SSLCertificateKeyFile /etc/pki/tls/private/server.key
    ServerAdmin # 2.1.2의 hostname
    DocumentRoot /var/www/html
    ServerName  # 2.1.2의 hostname
    ErrorLog logs/ssl_starkapin_com_error_log
    CustomLog logs/ssl_starkapin_com_error_log common
</VirtualHost>
```

- 서비스 적용을 위한 재시작

```
$ sudo service httpd restart
```

2.2.5 포트 방화벽 설정

- 수정 경로

```
$ sudo vi /etc/sysconfig/iptables
```

- 수정 사항

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
```

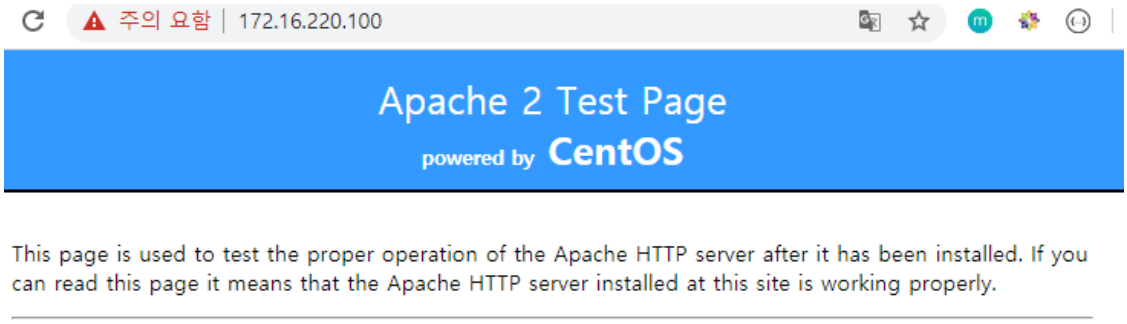
- 방화벽 재시작

```
$ sudo service iptables restart
```

2.2.6 SSL 적용 확인

- `https://IP` 접속 시

- 고급 - 안전하지 않음 이동 시



- 만약에 위와 같이 접속이 되지 않는다면 **방화벽 문제**이니 방화벽을 내리고 다시 시도하자.

```
$ sudo service iptables stop
```