

사이버 보안 Cyber Security

 Written by **Donghyun Choi (KGU)**


✂ - Worldskills Korea ▫ National 2025 (Cyber Security Practices) - 🕸 [Written by NullBins]

- By default, the commands are executed as a root user.

[Project-1] < Infrastructure configuration & Security enhancements >

☆ 추가 수정과제 (Revision Task)

1. 인증기관 구성 (Certificate-Authority Configuration)

-  인증기관(CA) 구축: 인증서 생성 및 Apache Tomcat 적용(OpenSSL 사용) 비대칭 RSA Signature 알고리즘 사용.

< Configuration >

- [server] : VM

```
nano /etc/ssl/openssl.cnf
```

```
[ CA_default ]
dir = /etc/ssl/0000-CA
x509_extensions = v3_req
policy = policy_anything

[ req_distinguished_name ]
countryName_default = KR
#stateOrProvinceName = Some-State
0.organizationName_default = 0000
```

```
nano /usr/lib/ssl/misc/CA.pl
```

```
my $CATOP = "/etc/ssl/0000-CA";
```

```
/usr/lib/ssl/misc/CA.pl -newca ✂ CN=0000-CA
cp /etc/ssl/0000-CA/cacert.pem /usr/local/share/ca-certificates/ca.crt
update-ca-certificates
cd /etc/ssl/0000-CA/certs/
```

```
openssl req -new -out server.req -newkey rsa:2048 -keyout server.key -nodes
✂ CN=192.168.127.129
openssl ca -in server.req -out server.crt
```

```
openssl req -new -out www.req -newkey rsa:2048 -keyout www.key -nodes
✂ CN=192.168.127.20
openssl ca -in server.req -out server.crt
```

```
cd /root/
docker cp www:/usr/local/tomcat/conf/server.xml ./
```

```
nano ./server.xml
```

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol"
    maxThreads="150" SSLEnabled="true"
    maxParameterCount="1000"
    >
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
    <SSLHostConfig>
        <Certificate certificateKeyFile="conf/www.key"
            certificateFile="conf/www.crt"
            certificateChainFile="conf/cacert.pem"
            type="RSA" />
    </SSLHostConfig>
</Connector>
```

```
docker cp /etc/ssl/0000-CA/certs/www.crt www:/usr/local/tomcat/conf/
docker cp /etc/ssl/0000-CA/certs/www.key www:/usr/local/tomcat/conf/
docker cp /etc/ssl/0000-CA/cacert.pem www:/usr/local/tomcat/conf/
docker cp ./server.xml www:/usr/local/tomcat/conf/
docker restart www
```

```
cd /home/kolo_user/apache-tomcat-9.0.89/
```

```
nano ./conf/server.xml
```

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true"
    maxParameterCount="1000"
    >
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />
    <SSLHostConfig>
        <Certificate certificateKeyFile="conf/server.key"
            certificateFile="conf/server.crt"
            certificateChainFile="conf/cacert.pem"
            type="RSA" />
    </SSLHostConfig>
</Connector>
```

```
cp /etc/ssl/0000-CA/certs/server.* ./conf/
cp /etc/ssl/0000-CA/cacert.pem ./conf/
./bin/shutdown.sh
./bin/startup.sh
```

< Checking >

- [HOST] -> Host Desktop PC

HOST-PC (Browser: Microsoft Edge)

<https://192.168.127.129:8443>

2025 SECURE BOARD

현재 DB 접속 상태 :

Board List

검색

번호	제목	태그	작성자	작성날짜	조회수
1	새로운 EDR 우회 기법, Babuk 랜섬웨어 설치에 이용	보안	admin	2025-05-30	0
2	SKT 해킹 이슈를 악용한 피싱 주의 권고	교육	admin	2025-05-30	0
3	아마존 AWS Amplify Studio 보안 업데이트 권고	일반	admin	2025-05-30	0
4	랜섬웨어 갱들, Skitnet 맬웨어로 스텔스 공격 활동 증가	교육	admin	2025-05-30	0
5	DragonForce 랜섬웨어, MSP를 통해 고객 시스템 공격	보안	admin	2025-05-30	0
6	로컬 DB 테스트	일반,교육	user01	2025-09-11	2

일반(G)

세부 정보(D)

발급 대상

CN(일반 이름) 192.168.127.129
조직 (O) 0000
OU(조직 구성 단위) <인증서의 일부가 아님>

발급자

CN(일반 이름) 0000-CA
조직 (O) 0000
OU(조직 구성 단위) 0000

유효 기간

발급 날짜 2025년 10월 4일 토요일 오후 11:27:05
만료 날짜 2026년 10월 4일 일요일 오후 11:27:05

SHA-256 지문

인증서 1b7eec01a36e29332e1eafe1fd6879cb339c730b56913d21305c4a0ac2b2c995
공개 키 ad2c3d3fbcca6441b8c873b41253b8748d433fdf86a386874b6ccdc4341c04b9

← ↻ 🏠 🔒 안전하지 않음 https://192.168.127.20:8443

☆ ⚙️ 👤 ... 🌐

2025 SECURE BOARD

현재 DB 접속 상태 :

Board List

--- ▾ 🔍

번호	제목	태그	작성자	작성날짜	조회수
1	새로운 EDR 우회 기법, Babuk 랜섬웨어 설치에 이용	보안	admin	2025-05-30	0
2	SKT 해킹 이슈를 악용한 피싱 주의 권고	교육	admin	2025-05-30	0
3	아마존 AWS Amplify Studio 보안 업데이트 권고	일반	admin	2025-05-30	0
4	랜섬웨어 갱들, Skitnet 맬웨어로 스텔스 공격 활동 증가	교육	admin	2025-05-30	0
5	DragonForce 랜섬웨어, MSP를 통해 고객 시스템 공격	보안	admin	2025-05-30	0
6	docker image test	일반,교육	user02	2025-09-10	1

일반(G)

세부 정보(D)

발급 대상

CN(일반 이름) 192.168.127.20

조직 (O) 0000

OU(조직 구성 단위) <인증서의 일부가 아님>

발급자

CN(일반 이름) 0000-CA

조직 (O) 0000

OU(조직 구성 단위) 0000

유효 기간

발급 날짜 2025년 10월 4일 토요일 오후 11:27:18

만료 날짜 2026년 10월 4일 일요일 오후 11:27:18

SHA-256 지문

인증서 6b0d20968b8a27f4c5091c0e24dc50bbe8f24842a5a48f75eed0c872356e588f

공개 키 c31a08c9d74e1251b2b6c9a5b707293a675f6d8df84f483467115129dbc48eca