Title: Securing Apache Web Server (Lab 5)

Omar faruk

Reg No: 2019831055

June 26, 2024

TASK-1: BECOMING A CERTIFICATE AUTHORITY (CA)

The first step for a secure web server is to setup an Apache web server. In your first web lab, you have already configured the Apache server for different virtual hosts: `example.com` and `webserverlab.com`. Before proceeding, ensure that you can access these virtual hosts using your preferred browser. You will secure these virtual hosts in today's lab by using TLS.

STEP 1: SETUP APACHE WEB SERVER

Verify Virtual Hosts: Ensure that you have already configured virtual hosts for `example.com` and `webserverlab.com`. You should be able to access these virtual hosts in your preferred browser.

STEP 2: CREATE A CA

Install OpenSSL: Ensure OpenSSL is installed on your machine.

Create Directory Structure:

```
mkdir myCA
cd myCA
mkdir newcerts
mkdir private
touch index.txt
echo 1000 > serial
```

Create OpenSSL Configuration File:

```
cp /usr/lib/ssl/openssl.cnf ./openssl.cnf
```

Generate a Self-Signed Certificate for the CA:

```
openssl req -new -x509 -days 3650 -keyout private/ca.key -out ca.crt -config openssl.cnf
```

Fill in the necessary information and create a strong passphrase.

Task-2: Generating and Signing Certificates for example.com

Step 1: Generate Public/Private Key Pair for example.com

Generate RSA Key Pair:

```
openssl genrsa -des3 -out example.com.key 2048
```

Step 2: Generate a Certificate Signing Request (CSR)

Create CSR:

```
openssl req -new -key example.com.key -out example.com.csr -config openssl.cnf
```

Step 3: Sign the CSR with the CA

Sign CSR to Generate Certificate:

```
openssl ca -in example.com.csr -out example.com.crt -cert ca.crt -keyfile private/ca.key -
    config openssl.cnf
```

Task-3: Deploy HTTPS into Apache

Step 1: Configure Apache for SSL

Edit Virtual Host Configuration: Add the following lines to `/etc/apache2/sites-available/example.com.c`

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerAdmin admin@example.com
        ServerName example.com
        ServerAlias www.example.com
        DocumentRoot /var/www/example.com/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /path/to/example.com.crt
        SSLCertificateKeyFile /path/to/example.com.key
    </VirtualHost>
</IfModule>
```

Enable SSL Module in Apache:

```
sudo a2enmod ssl
```

Test Apache Configuration:

```
sudo apache2ctl configtest
```

Restart Apache:

```
sudo systemctl restart apache2
```

Step 2: Accessing the Secured Site

Access the Site: Open your browser and go to `https://example.com`. If you see a security warning, manually import the CA certificate (`ca.crt`) into your browser.